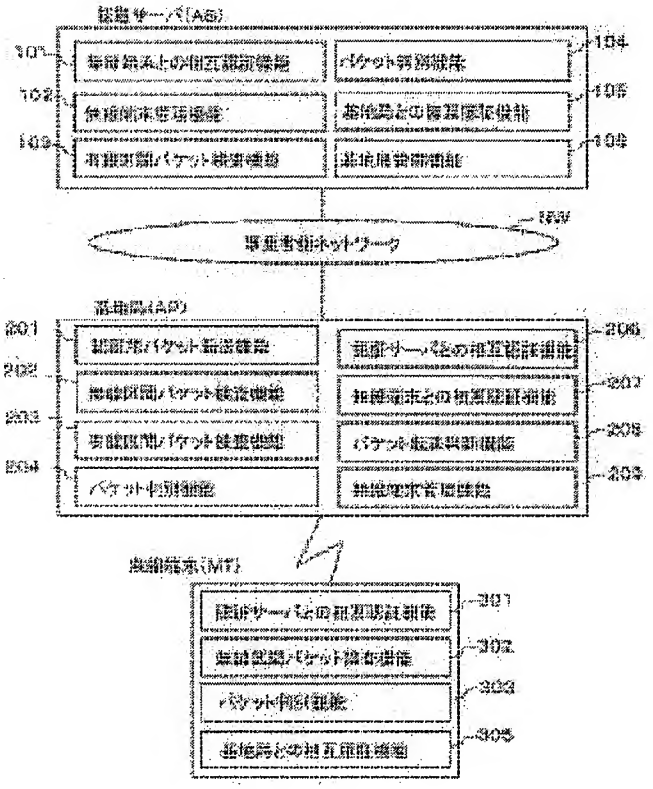
RADIO ACCESS NETWORK, MULTIHOPPING RADIO NETWORK, AUTHENTICATION SERVER, BASE STATION AND RADIO TERMINAL

Publication number: JP2003249944 (A)
Publication date: 2003-09-05
Inventor(s): NIHEI KATSUTOSHI; YOSHINO SHUICHI; NAKAYAMA MASAYOSHI; SUDA HIROTO
Applicant(s): NIPPON TELEGRAPH & TELEPHONE
Classification:
- international: ***H04L9/32; H04L12/56; H04Q7/38;*** **H04L9/32; H04L12/56; H04Q7/38;** (IPC1-7): H04L12/56; H04L9/32; H04Q7/38
- European:
Application number: JP20020045240 20020221
Priority number(s): JP20020045240 20020221

Also published as:
JP3880419 (B2)

Abstract of **JP 2003249944 (A)**

PROBLEM TO BE SOLVED: To provide a technique having excellent resistance to a DoS (Denial of Service) attack in a radio access network and a multihopping radio network.



(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2003－249944
（P2003－249944A）
(43)公開日　平成15年９月５日(2003.9.5)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　12/56		Ｈ０４Ｌ　12/56	Ａ	５Ｊ１０４
9/32		9/00	６７５Ｄ	５Ｋ０３０
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｒ	５Ｋ０６７

審査請求　未請求　請求項の数18　ＯＬ　（全 42 頁）

(21)出願番号　特願2002－45240(P2002－45240)

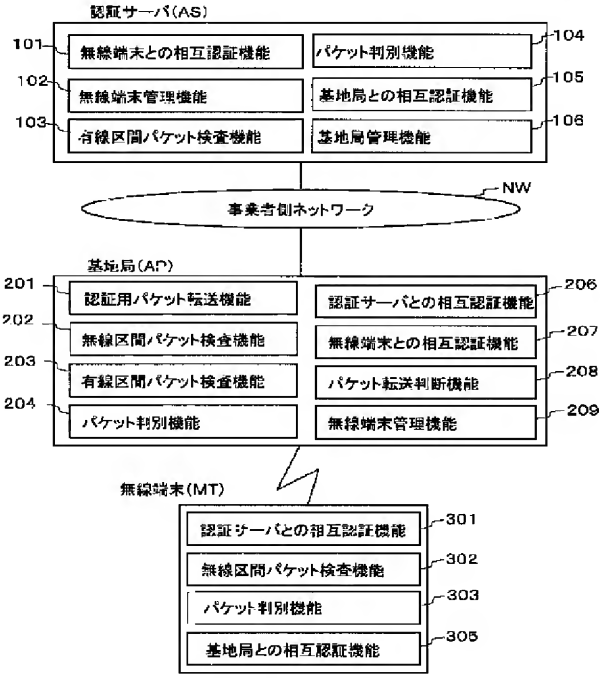
(22)出願日　平成14年２月21日(2002.2.21)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(72)発明者　仁平　勝利
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　吉野　修一
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(74)代理人　100083806
弁理士　三好　秀和　（外１名）

最終頁に続く

(54)【発明の名称】　無線アクセスネットワーク、無線マルチホップネットワーク、認証サーバ、基地局及び無線端末

(57)【要約】
【課題】　無線アクセスネットワーク、無線マルチホップネットワークにおいて、ＤｏＳ攻撃に対する耐性に優れた技術を提供する。
【解決手段】　認証サーバ（ＡＳ）と新規な基地局（ＡＰ）が相互認証を行うことで、事業者が一般ユーザの設置したＡＰの安全性を保障する。また新規無線端末（ＭＴ）がアクセスしたとき、最初にＭＴ－ＡＰ間で相互認証することで互いが正当な装置であるか否かを確認し、ＡＰはこの相互認証が成功するまでは新規ＭＴが送信したパケットを事業者側ネットワークに転送しないようにすることにより、認証を装ったＤｏＳ攻撃を防止する。さらに、ＭＴ－ＡＰ間の相互認証成功後にＭＴ－ＡＳ間の相互認証及びこの認証用パケットのパケット検査（送信元確認）を行うことでＡＳはどのＡＰにどのＭＴがアクセスしたかを正確に把握する。



【特許請求の範囲】
【請求項１】　無線端末と、この無線端末との間で無線通信する基地局と、この基地局と事業者側ネットワークで接続された認証サーバとから構成される無線アクセスネットワークにおいて、
Ａ．前記基地局は、前記事業者側ネットワークに新規に接続するときに基地局－認証サーバ間認証用パケットを送信して前記認証サーバと相互認証を行う処理機能、
Ｂ．前記無線端末は、当該無線アクセスネットワークに新規にアクセスするときに近隣にある基地局と相互認証を行い、認証成功後に無線端末－認証サーバ間認証用パケットを送信し、前記基地局は、前記無線端末との相互認証が成功したときに当該無線端末から送信されてきた前記無線端末－認証サーバ間認証用パケットの転送を許可し、前記認証サーバは、前記無線端末－認証サーバ間認証用パケットにより前記基地局を介して前記無線端末と相互認証を行う処理機能、
Ｃ．前記無線端末、基地局、認証サーバそれぞれは、前記無線端末－認証サーバ間認証用パケットを送信し又は転送するときに送信元を示すパケット検査データを当該認証用パケットに添付する処理機能、
Ｄ．前記無線端末、基地局、認証サーバそれぞれは、前記無線端末－認証サーバ間認証用パケットを受信したときに、それに添付されているパケット検査データを検査し、当該検査が失敗した場合はそれが添付されている認証用パケットを破棄する処理機能、
Ｅ．前記認証サーバは認証した新規の基地局、新規の無線端末それぞれの情報を自装置に登録する処理機能を備えたことを特徴とする無線アクセスネットワーク。
【請求項２】　中継能力を持つ無線端末と、この無線端末と無線通信する基地局と、この基地局と事業者側ネットワークを通じて接続される認証サーバとから構成される無線マルチホップネットワークにおいて、
Ａ．前記基地局は、新規に事業者側ネットワークに接続するときに前記認証サーバと基地局－認証サーバ間認証パケットを用いて相互認証を行う処理機能、
Ｂ．前記無線端末は、新規に当該無線マルチホップネットワークにアクセスするときに近隣の認証済みの無線端末又は基地局と無線端末間認証用パケットによって相互認証を行う処理機能、
Ｃ．前記無線端末間の相互認証が成功した無線端末又は基地局が複数あれば、その中から１つの無線端末又は基地局を選択し、前記選択された無線端末又は基地局は、前記新規無線端末から送信された無線端末－認証サーバ間認証用パケットの転送を許可する処理機能、
Ｄ．前記新規無線端末は、前記無線端末間の相互認証の成功後に、無線端末－認証サーバ間認証用パケットを用い、選択した無線端末又は基地局を経由して前記認証サーバと相互認証を行う処理機能、
Ｅ．前記新規無線端末、選択された無線端末、基地局、認証サーバそれぞれは、前記無線端末－認証サーバ間認証用パケットを送信し又は転送するときに送信元を示すパケット検査データを当該認証用パケットに添付する処理機能、
Ｆ．前記新規無線端末、選択された無線端末、基地局、認証サーバそれぞれは、前記無線端末－認証サーバ間認証用パケットを受信したときに、それに添付されているパケット検査データを検査し、当該検査が失敗した場合はそれが添付されている認証用パケットを破棄する処理機能、
Ｇ．前記認証サーバは相互認証に成功した新規の基地局、新規の無線端末それぞれの情報を自装置に登録する処理機能を備えたことを特徴とする無線マルチホップネットワーク。
【請求項３】　無線端末と、この無線端末との間で無線通信する基地局と、この基地局と事業者側ネットワークで接続された認証サーバとから構成される無線アクセスネットワークに用いられる無線端末であって、
前記無線アクセスネットワークに新規にアクセスするときに、無線端末－基地局間認証用パケットを送信して近隣の基地局と相互認証を行い、認証成功後に無線端末－認証サーバ間認証用パケットを送信し、認証サーバとの間で相互認証を行う機能を備えたことを特徴とする無線端末。
【請求項４】　送信する無線端末－認証サーバ間認証用パケットに送信元を示すパケット検査データを算出して添付する機能を備えた請求項３に記載の無線端末。
【請求項５】　前記無線端末－基地局間認証用パケットを送信し、複数の基地局から応答を受けたとき、無線端末－基地局間認証において正当な１つの基地局を選択し、当該基地局を通じて前記無線端末－認証サーバ間認証用パケットを前記認証サーバに送信する機能を備えたことを特徴とする請求項３又は４に記載の無線端末。
【請求項６】　前記無線端末－基地局間認証用パケットを送信し、複数の基地局から応答を受けたとき、応答の早い基地局から優先的に選択して無線端末－基地局間認証を実行する機能を備えたことを特徴とする請求項５に記載の無線端末。
【請求項７】　前記無線端末－基地局間認証用パケットを送信し、複数の基地局から応答を受けたとき、応答信号の受信レベルの強い基地局から優先的に選択して無線端末－基地局間認証を実行する機能を備えたことを特徴とする請求項５に記載の無線端末。
【請求項８】　前記無線端末－基地局間認証用パケットを送信し、複数の基地局から応答を受けたとき、各基地局間との無線端末－基地局間の認証手続きにおいて取得した情報に基づき、正当な基地局を選択する機能を備えたことを特徴とする請求項５に記載の無線端末。
【請求項９】　無線端末と、この無線端末との間で無線通信する基地局と、この基地局と事業者側ネットワーク

で接続された認証サーバとから構成される無線アクセスネットワーク又は無線マルチアクセスネットワークに用いられる認証サーバであって、
新規にアクセスしてきた基地局と相互認証を実行し、認証が成功した基地局の情報を自装置に登録する機能と、無線端末－認証サーバ間認証用パケットにパケット検査データを添付して基地局に送信し、基地局から送られてきた無線端末－認証サーバ間認証用パケットに添付されているパケット検査データを検査し、検査が失敗した場合はそのパケットを破棄し、この検査が成功すれば無線端末との相互認証を実施し、相互認証に成功した無線端末の情報を自装置に登録する機能を備えたことを特徴とする認証サーバ。
【請求項１０】　相互認証に成功した無線端末が別の基地局の通信エリアへ移動したとき、当該無線端末との新たな相互認証を実施し、認証が成功した後に当該無線端末の属していた旧基地局へその無線端末が移動したことを通知する機能を備えたことを特徴とする請求項９に記載の認証サーバ。
【請求項１１】　無線端末と、この無線端末との間で無線通信する基地局と、この基地局と事業者側ネットワークで接続された認証サーバとから構成される無線アクセスネットワーク又は無線マルチホップネットワークにおいて用いられる基地局であって、
新規に前記無線アクセスネットワーク又は無線マルチホップネットワークに接続したときに、基地局－認証サーバ間認証用パケットを前記認証サーバに送信して相互認証を実行する機能を備えたことを特徴とする基地局。
【請求項１２】　新規の無線端末からの無線端末－基地局間認証要求に対して相互認証を行い、当該相互認証が成功したときに当該無線端末から送信されてきた無線端末－認証サーバ間認証用パケットに対して、それに添付されているパケット検査データを検査し、検査が失敗した場合はそのパケットを破棄し、当該検査が成功すれば、当該無線端末－認証サーバ間認証用パケットを、自装置で算出したパケット検査データを添付して認証サーバに転送し、認証サーバから送信されてきた認証用パケットに示されている認証結果を参照して新規無線端末が送信したすべてのパケットの事業者側ネットワークへの転送を許可するか否かを判定する機能を備えたことを特徴とする請求項１１に記載の基地局。
【請求項１３】　相互認証に成功した無線端末それぞれの情報を自装置に登録する機能と、認証サーバから移動通知を受けて、該当する無線端末の登録情報を削除する機能とを備えたことを特徴とする請求項１１又は１２に記載の基地局。
【請求項１４】　中継能力を持つ無線端末と、この無線端末と無線通信する基地局と、この基地局と事業者側ネットワークを通じて接続される認証サーバとから構成される無線マルチホップネットワークにおいて用いられる無線端末であって、
自装置が新規に無線マルチホップネットワークにアクセスするときには近隣の認証済みの他の無線端末又は基地局と相互認証を行い、複数の無線端末又は基地局と相互認証が成功した場合、正当な１つの無線端末又は基地局をプロキシ端末として選択し、当該プロキシ端末を介して認証サーバとの相互認証を実行する機能と、
自装置が他の新規無線端末によって選択されたプロキシ端末である場合には、他の新規無線端末から送信された新規無線端末－認証サーバ間認証用パケットをルート上の他の無線端末又は基地局に対して転送する機能とを備えたことを特徴とする無線端末。
【請求項１５】　自装置が新規に無線マルチホップネットワークにアクセスするときに、無線端末間認証用パケットを近隣の他の無線端末又は基地局に送信する機能と、
自装置が新規無線端末である場合に、無線端末－認証サーバ間認証用パケットに送信元を示すパケット検査データを添付して送信する機能と、
自装置が他の新規無線端末によって選択されたプロキシ端末である場合には、他の新規無線端末又は基地局から送信された無線端末－認証サーバ間認証用パケットに対してパケット検査データを検査し、検査が失敗すればその認証用パケットを破棄し、当該検査が成功すれば当該認証用パケットに自装置で算出した送信元を示すパケット検査データを添付してルート上の他の無線端末又は基地局に対して転送する機能とを備えたことを特徴とする請求項１４に記載の無線端末。
【請求項１６】　基地局又は他の無線端末に対する相互認証要求に対して複数の他の無線端末又は基地局から応答を受けたとき、応答の早い基地局又は他の無線端末から優先的にプロキシ端末として選択する機能を備えたことを特徴とする請求項１４又は１５に記載の無線端末。
【請求項１７】　基地局又は他の無線端末に対する相互認証要求に対して複数の他の無線端末又は基地局から応答を受けたとき、受信レベルの強い基地局又は他の無線端末から優先的にプロキシ端末として選択する機能を備えたことを特徴とする請求項１４又は１５に記載の無線端末。
【請求項１８】　基地局又は他の無線端末に対する相互認証要求に対して複数の他の無線端末又は基地局から応答を受けたとき、相互認証で取得した他の無線端末又は基地局の情報に基づいてプロキシ端末を選択する機能を備えたことを特徴とする請求項１４又は１５に記載の無線端末。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は基地局を介して有線ネットワークに接続される無線アクセスネットワーク又は無線マルチホップネットワークにおいて、無線端末及

び基地局の認証を行う認証方法に関するものである。
【０００２】
【従来の技術】図５０に認証サーバ（ＡＳ：Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｓｅｒｖｅｒ）を用いた無線アクセスネットワークの一般的な機能構成を示してある。この無線アクセスネットワークは、無線端末ＭＴ（Ｍｏｂｉｌｅ　Ｔｅｒｍｉｎａｌ）、この無線端末ＭＴと無線通信する基地局ＡＰ（Ａｃｃｅｓｓ　Ｐｏｉｎｔ）、この基地局ＡＰと事業者側有線ネットワークＮＷを通じて接続される認証サーバＡＳから構成される。
【０００３】認証サーバＡＳはソフトウェアとして、無線端末ＭＴとの相互認証を実行する無線端末との認証機能１０１、認証した無線端末ＭＴをデータベースに登録して管理する無線端末管理機能１０２、ネットワークＮＷのパケットを検査する有線区間パケット検査機能１０３、パケット判別を行うパケット判別機能１０４を備えている。
【０００４】基地局ＡＰはソフトウェアとして、認証サーバＡＳ－無線端末ＭＴ間の認証用パケットの転送を行う認証用パケット転送機能２０１、無線ネットワークのパケットを検査する無線区間パケット検査機能２０２、有線ネットワークＮＷのパケットを検査する有線区間パケット検査機能２０３、パケット判別を行うパケット判別機能２０４を備えている。
【０００５】無線端末ＭＴはソフトウェアとして、認証サーバＡＳとの相互認証を実行する認証サーバとの相互認証機能３０１、無線ネットワークのパケットを検査する無線区間パケット検査機能３０２、パケット判別を行うパケット判別機能３０３を備えている。
【０００６】この提案されている無線アクセスネットワークでは、ある無線端末ＭＴがそのネットワークにアクセスするとき、ＭＴは基地局ＡＰを介してＡＳと相互認証を行う。基地局ＡＰは、無線端末ＭＴから受信した認証用パケットを終端して認証サーバＡＳへ転送し、また認証サーバＡＳから受信した認証用パケットを無線端末ＭＴへ転送する。認証サーバＡＳによる無線端末ＭＴの認証が成功したら、基地局ＡＰに対してそのＭＴから無線送信されてきたデータパケットを事業者側ネットワークＮＷへの転送を許可し、無線端末ＭＴから事業者用ネットワークＮＷ上の他の接続端末へのアクセスを可能にする。
【０００７】
【発明が解決しようとする課題】このような無線アクセスネットワークでは、基地局ＡＰが会社内等の限定されたアクセス環境ではなく、屋外等の誰でも容易にアクセスできる環境に設置されることが特徴であるが、そのような場合は、図５１に示したように、悪意あるユーザが無線端末ＭＴの認証を装って大量にパケットを送信することによって認証サーバＡＳをダウンさせることが可能である。このようなＤｅｎｉａｌ　ｏｆＳｅｒｖｉｃｅ（ＤｏＳ）攻撃をされた場合、その無線アクセスネットワークへ新規ユーザが無線端末ＭＴによってアクセスすることが不可能になる。
【０００８】一方、事業者ではなく、一般ユーザが基地局ＡＰを設置した場合、認証サーバＡＳでは新規の基地局ＡＰの認証を行わないため、事業者がそうしたＡＰのセキュリティ機能を保障することが不可能となる。そのため、一般ユーザが設置したＡＰには、他ユーザが安心してアクセスすることができない。その上、基地局ＡＰの認証がない場合、基地局ＡＰから送信されたトラヒック情報や課金情報等の正当性も確認できないので問題となる。
【０００９】また、一般ユーザが基地局ＡＰを設置した場合、図５２に示したように、ＡＰの設置密度が高くなって１つの無線端末ＭＴが複数の基地局ＡＰ＃ｉとＡＰ＃ｊとに同時にアクセス可能になることも考えられる。こうした環境では、無線端末ＭＴが同時に複数のＡＰを介して認証サーバと認証を行うことになり、同じ認証処理が同時に発生してしまう問題がある。
【００１０】この同時認証処理が発生する問題は、各々の無線端末ＭＴが中継機能を持つ無線マルチホップネットワークにおいて顕著となる。図５３に無線マルチホップネットワークの機能構成例を示してある。この無線マルチホップネットワークでは、基地局ＡＰがパケット中継機能２０５を追加的に備え、また無線端末ＭＴもパケット中継機能３０４を追加的に備えている。そして、図５３に示した無線マルチホップネットワークでは、例えば、無線端末ＭＴ７は、他の無線端末ＭＴ６，ＭＴ４に中継されて基地局ＡＰ１にアクセスし、この基地局ＡＰ１からネットワークＮＷを通じて認証サーバＡＳに接続され、またその逆の径路でＡＳから無線端末ＭＴ７と通信する。
【００１１】このような無線マルチホップネットワークでは、新規無線端末ＭＴは認証前には基地局ＡＰまでの経路情報を保持していないので、認証要求をブロードキャストで送信する。この場合、新規ＭＴの近隣の複数のＭＴが認証要求を受信し、それぞれがその認証要求を基地局に通じる次のＭＴへ中継する。この結果として、同じ認証処理が同時に発生することになる。
【００１２】図５４に無線マルチホップネットワークにおける認証時の問題を示す。無線端末ＭＴ９が新規ＭＴの認証を装ってＤｏＳ攻撃をかけた場合、この無線端末ＭＴ９からブロードキャストで送り出される信号を図示では複数の無線端末ＭＴ５，ＭＴ６，ＭＴ７が同時に受信し、これらの無線端末がさらに他の無線端末を通じて複数の基地局ＡＰ＃ｉ，ＡＰ＃ｊにアクセスし、これから認証サーバＡＳに認証要求を同時に送信することになり、無線マルチホップネットワーク上に不正なパケットが流入し、他のパケットの転送が妨害されることになるのである。

【００１３】本発明は、このような提案されている無線アクセスネットワーク、無線マルチホップネットワークにおいて、ＤｏＳ攻撃に対する耐性に優れた技術を提供することを目的とする。

【００１４】

【課題を解決するための手段】請求項１の発明は、無線端末と、この無線端末との間で無線通信する基地局と、この基地局と事業者側ネットワークで接続された認証サーバとから構成される無線アクセスネットワークにおいて、

Ａ．前記基地局は、前記事業者側ネットワークに新規に接続するときに基地局－認証サーバ間認証用パケットを送信して前記認証サーバと相互認証を行う処理機能、

Ｂ．前記無線端末は、当該無線アクセスネットワークに新規にアクセスするときに近隣にある基地局と相互認証を行い、認証成功後に無線端末－認証サーバ間認証用パケットを送信し、前記基地局は、前記無線端末との相互認証が成功したときに当該無線端末から送信されてきた前記無線端末－認証サーバ間認証用パケットの転送を許可し、前記認証サーバは、前記無線端末－認証サーバ間認証用パケットにより前記基地局を介して前記無線端末と相互認証を行う処理機能、

Ｃ．前記無線端末、基地局、認証サーバそれぞれは、前記認証用パケットそれぞれを送信し又は転送するときに送信元を示すパケット検査データを当該認証用パケットに添付する処理機能、

Ｄ．前記無線端末、基地局、認証サーバそれぞれは、前記無線端末－認証サーバ間認証用パケットを受信したときに、それに添付されているパケット検査データを検査し、当該検査が失敗した場合はそれが添付されている認証用パケットを破棄する処理機能、

Ｅ．前記認証サーバは認証した新規の基地局、新規の無線端末それぞれの情報を自装置に登録する処理機能を備えたものである。

【００１５】請求項１の発明の無線アクセスネットワークでは、認証サーバ（ＡＳ）と基地局（ＡＰ）が相互認証を行うことで、事業者が一般ユーザの設置したＡＰの安全性を保障することが可能となる。新規無線端末（ＭＴ）がアクセスしたとき、最初にＭＴ－ＡＰ間で相互認証することで互いが正当な装置であるか否かを確認することができ、ＡＰはこの相互認証が成功するまでは新規ＭＴが送信したパケットを事業者側ネットワークに転送しないので、認証を装ったＤｏＳ攻撃を防止することができる。

【００１６】ＭＴ－ＡＰ間の相互認証成功後にＭＴ－ＡＳ間の相互認証及びこの認証用パケットのパケット検査（送信元確認）を行うことでＡＳはどのＡＰにどのＭＴがアクセスしたかを正確に把握して管理することが可能となる。

【００１７】請求項２の発明は、中継能力を持つ無線端末と、この無線端末と無線通信する基地局と、この基地局と事業者側ネットワークを通じて接続される認証サーバとから構成される無線マルチホップネットワークにおいて、

Ａ．前記基地局は、新規に事業者側ネットワークに接続するときに前記認証サーバと基地局－認証サーバ間認証パケットを用いて相互認証を行う処理機能、

Ｂ．前記無線端末は、新規に当該無線マルチホップネットワークにアクセスするときに近隣の認証済みの無線端末又は基地局と無線端末間認証用パケットによって相互認証を行う処理機能、

Ｃ．前記無線端末間の相互認証が成功した無線端末又は基地局が複数あれば、その中から１つの無線端末又は基地局を選択し、前記選択された無線端末又は基地局は、前記新規無線端末から送信された無線端末－認証サーバ間認証用パケットの転送を許可する処理機能、

Ｄ．前記新規無線端末は、前記無線端末間の相互認証の成功後に、無線端末－認証サーバ間認証用パケットを用い、選択した無線端末又は基地局を経由して前記認証サーバと相互認証を行う処理機能、

Ｅ．前記新規無線端末、選択された無線端末、基地局、認証サーバそれぞれは、前記無線端末－認証サーバ間認証用パケットを送信し又は転送するときに送信元を示すパケット検査データを当該認証用パケットに添付する処理機能、

Ｆ．前記新規無線端末、選択された無線端末、基地局、認証サーバそれぞれは、前記認証用パケットそれぞれを受信したときに、それに添付されているパケット検査データを検査し、当該検査が失敗した場合はそれが添付されている認証用パケットを破棄する処理機能、

Ｇ．前記認証サーバは相互認証に成功した新規の基地局、新規の無線端末それぞれの情報を自装置に登録する処理機能を備えたものである。

【００１８】請求項２の発明の無線マルチホップネットワークでは、新規無線端末（ＭＴ）が無線マルチホップネットワークにアクセスしたとき、最初に新規ＭＴ－近隣ＭＴ間で相互認証することで互いが正当な装置であるか否かを確認することができ、近隣のＭＴはこの相互認証が成功するまでは新規ＭＴが送信したパケットを無線マルチホップネットワークに転送しないので、認証を装ったＤｏＳ攻撃を防止することができる。

【００１９】また、相互認証の際にＭＴ－ＡＳ（認証サーバ）間相互認証用パケットを中継させるＭＴ又はＡＰ（基地局）を１つ選択することで、同じ認証処理が同時に複数発生してしまうことを防止する。

【００２０】さらに、ＭＴ－ＡＰ間の相互認証成功後にＭＴ－ＡＳ間の相互認証及びこの認証用パケットのパケット検査（送信元確認）を行うことでＡＳはどのＡＰにどのＭＴがアクセスしたかを正確に把握して管理することが可能となる。

【００２１】請求項３の発明は、無線端末と、この無線端末との間で無線通信する基地局と、この基地局と事業者側ネットワークで接続された認証サーバとから構成される無線アクセスネットワークに用いられる無線端末であって、前記無線アクセスネットワークに新規にアクセスするときに、無線端末－基地局間認証用パケットを送信して近隣の基地局と相互認証を行い、認証成功後に無線端末－認証サーバ間認証用パケットを送信し、認証サーバとの間で相互認証を行う機能を備えたものである。

【００２２】請求項３の発明の無線端末（ＭＴ）では、無線アクセスネットワークに新規に参入するときに基地局（ＡＰ）と相互認証を行い、その成功の後に認証サーバ（ＡＳ）と相互認証を行う機能を備えたことで、ＡＰに新規ＭＴとの相互認証が成功するまで新規ＭＴの送信したパケットを事業者側ネットワークに転送しない機能を持たせることによって、当該ＭＴを用いなければＡＰとの通信、ひいては認証サーバ（ＡＳ）との通信ができない無線アクセスネットワークを構築することができ、認証を装ったＤｏＳ攻撃に耐性の強い無線アクセスネットワークの構築に寄与できる。

【００２３】請求項４の発明は、請求項３の無線端末において、送信する無線端末－認証サーバ間認証用パケットに送信元を示すパケット検査データを算出して添付する機能を備えたものであり、無線端末－認証サーバ間認証用パケットにパケット検査データを添付することにより、受信先の基地局に送信元を明かすことができ、不正な攻撃のために用いられなくできる。

【００２４】請求項５の発明は、請求項３又は４の無線端末において、前記無線端末－基地局間認証用パケットを送信し、複数の基地局から応答を受けたとき、無線端末－基地局間認証において正当な１つの基地局を選択し、当該基地局を通じて前記無線端末－認証サーバ間認証用パケットを前記認証サーバに送信する機能を備えたものである。

【００２５】請求項６の発明は、請求項５の無線端末において、前記無線端末－基地局間認証用パケットを送信し、複数の基地局から応答を受けたとき、応答の早い基地局から優先的に選択して無線端末－基地局間認証を実行する機能を備えたものである。

【００２６】請求項７の発明は、請求項５の無線端末において、前記無線端末－基地局間認証用パケットを送信し、複数の基地局から応答を受けたとき、応答信号の受信レベルの強い基地局から優先的に選択して無線端末－基地局間認証を実行する機能を備えたものである。

【００２７】請求項８の発明は、請求項５の無線端末において、前記無線端末－基地局間認証用パケットを送信し、複数の基地局から応答を受けたとき、各基地局間との無線端末－基地局間の認証手続きにおいて取得した情報に基づき、正当な基地局を選択する機能を備えたものである。

【００２８】請求項５～８の発明の無線端末（ＭＴ）では、新規ＭＴはＭＴ－ＡＰ（基地局）間相互認証の際にＭＴ－ＡＳ（認証サーバ）間相互認証用パケットを中継させるＡＰ又はＭＴを所定のロジックにしたがって選択することで、同じ認証処理が同時に複数発生してしまうことを防止することができる。

【００２９】請求項９の発明は、無線端末と、この無線端末との間で無線通信する基地局と、この基地局と事業者側ネットワークで接続された認証サーバとから構成される無線アクセスネットワーク又は無線マルチアクセスネットワークに用いられる認証サーバであって、新規にアクセスしてきた基地局と相互認証を実行し、認証が成功した基地局の情報を自装置に登録する機能と、無線端末－認証サーバ間認証用パケットにパケット検査データを添付して基地局に送信し、基地局から送られてきた無線端末－認証サーバ間認証用パケットに添付されているパケット検査データを検査し、検査が失敗した場合はそのパケットを破棄し、この検査が成功すれば無線端末との相互認証を実施し、相互認証に成功した無線端末の情報を自装置に登録する機能を備えたものである。

【００３０】請求項９の発明の認証サーバ（ＡＳ）では、基地局（ＡＰ）と相互認証を行い、また新規無線端末（ＭＴ）とも相互認証を行い、しかも新規無線端末との相互認証の際に認証用パケットに添付されている送信元を示すパケット検査データを検査し、この検査が成功すれば相互認証を実施することになるので、不正なＡＰを排除し、正規のＡＰだけを管理することができ、またどのＡＰにどのＭＴがアクセスしたかをも正確に把握することが可能となる。

【００３１】請求項１０の発明は、請求項９の認証サーバにおいて、相互認証に成功した無線端末が別の基地局の通信エリアへ移動したとき、当該無線端末との新たな相互認証を実施し、認証が成功した後に当該無線端末の属していた旧基地局へその無線端末が移動したことを通知する機能を備えたものである。

【００３２】請求項１０の発明の認証サーバ（ＡＳ）では、自身の認証した無線端末（ＭＴ）の移動を管理し、ＭＴがある基地局（ＡＰ）から別のＡＰへ移動した時、ＭＴ－ＡＳ間の相互認証が成功した後に、そのＭＴが属していた旧ＡＰへ当該ＭＴが移動したことを通知することにより、ＡＰに一度は相互認証したがいまでは移動して通信できなくなったＭＴの記録をいつまでも保持させなくてもよく、ＡＰにおけるＭＴの管理データを少なくでき、それだけ処理の高速化が図れる。

【００３３】請求項１１の発明は、無線端末と、この無線端末との間で無線通信する基地局と、この基地局と事業者側ネットワークで接続された認証サーバとから構成される無線アクセスネットワーク又は無線マルチホップネットワークにおいて用いられる基地局であって、新規に前記無線アクセスネットワーク又は無線マルチホップ

ネットワークに接続したときに、基地局－認証サーバ間認証用パケットを前記認証サーバに送信して相互認証を実行する機能を備えたものである。

【００３４】請求項１１の発明の基地局（ＡＰ）では、新規に無線アクセスネットワーク又は無線マルチホップネットワークに接続するときには必ず認証サーバと相互認証を実施するため、不正にＡＰを設置することを困難にし、事業者が一般ユーザの設置したＡＰの安全性を保障することが可能となる。

【００３５】請求項１２の発明は、請求項１１の基地局において、新規の無線端末からの無線端末－基地局間認証要求に対して相互認証を行い、当該相互認証が成功したときに当該無線端末から送信されてきた無線端末－認証サーバ間認証用パケットに対して、それに添付されているパケット検査データを検査し、検査が失敗した場合はそのパケットを破棄し、当該検査が成功すれば、当該無線端末－認証サーバ間認証用パケットに自装置で算出したパケット検査データを添付して認証サーバに転送し、認証サーバから送信されてきた認証用パケットに示されている認証結果を参照して新規無線端末が送信したすべてのパケットの事業者側ネットワークへの転送を許可するか否かを判定する機能を備えたことを特徴とするものである。

【００３６】請求項１２の発明の基地局（ＡＰ）では、新規無線端末（ＭＴ）がアクセスしてきたとき、最初にＭＴ－ＡＰ間で相互認証することでＭＴが正当な装置であるか否かを確認し、この相互認証が成功するまでは新規ＭＴが送信したパケットを事業者側ネットワークに転送しないので、認証を装ったＤｏＳ攻撃を防止することができる。

【００３７】請求項１３の発明は、請求項１１又は１２の基地局において、相互認証に成功した無線端末それぞれの情報を自装置に登録する機能と、認証サーバから移動通知を受けて、該当する無線端末の登録情報を削除する機能とを備えたものであり、無線端末が他の基地局の通信エリアに移動した場合に、通信ができなくなってしまった無線端末の情報を削除することによって無線端末の管理のためのリソースを節約できる。

【００３８】請求項１４の発明は、中継能力を持つ無線端末と、この無線端末と無線通信する基地局と、この基地局と事業者側ネットワークを通じて接続される認証サーバとから構成される無線マルチホップネットワークにおいて用いられる無線端末であって、自装置が新規に無線マルチホップネットワークにアクセスするときには近隣の認証済みの他の無線端末又は基地局と相互認証を行い、複数の無線端末又は基地局と相互認証が成功した場合、正当な１つの無線端末又は基地局をプロキシ端末として選択し、当該プロキシ端末を介して認証サーバとの相互認証を実行する機能と、自装置が他の新規無線端末によって選択されたプロキシ端末である場合には、他の新規無線端末から送信された新規無線端末－認証サーバ間認証用パケットをルート上の他の無線端末又は基地局に対して転送する機能とを備えたものである。

【００３９】請求項１４の発明の無線端末（ＭＴ）では、無線マルチホップネットワークに新規にアクセスするとき、最初に近隣ＭＴ又はＡＰとの間で相互認証する機能を備えたことで、当該ＭＴが新規に無線マルチホップネットワークに参入する際には近隣のＭＴ又はＡＰに正当な装置であるか否かを確認させ、近隣のＭＴ又はＡＰはこの相互認証が成功するまでは当該ＭＴが送信したパケットを無線マルチホップネットワークに転送しないので、認証を装ったＤｏＳ攻撃に対する耐性の高い無線マルチホップネットワークの構築に寄与できる。

【００４０】請求項１４の発明の無線端末（ＭＴ）ではまた、相互認証の際にＭＴ－ＡＳ（認証サーバ）間相互認証用パケットを中継させるＭＴ又はＡＰ（基地局）を１つ選択する機能を備えたことで、同じ認証処理が同時に複数発生してしまうことを防止する。

【００４１】請求項１５の発明は、請求項１４の無線端末において、自装置が新規に無線マルチホップネットワークにアクセスするときに、無線端末間認証用パケットを近隣の他の無線端末又は基地局に送信する機能と、自装置が新規無線端末である場合に、無線端末－認証サーバ間認証用パケットに送信元を示すパケット検査データを添付して送信する機能と、自装置が他の新規無線端末によって選択されたプロキシ端末である場合には、他の新規無線端末から送信された無線端末－認証サーバ間認証用パケットに対してパケット検査データを検査し、検査が失敗すればその認証用パケットを破棄し、当該検査が成功すれば当該認証用パケットに自装置で算出した送信元を示すパケット検査データを添付してルート上の他の無線端末又は基地局に対して転送する機能とを備えたものであり、どの基地局（ＡＰ）にどの無線端末（ＭＴ）がアクセスしたかを認証サーバに正確に把握させることができる。

【００４２】請求項１６の発明は、請求項１４又は１５の無線端末において、基地局又は他の無線端末に対する相互認証要求に対して複数の他の無線端末又は基地局から応答を受けたとき、応答の早い基地局又は他の無線端末から優先的にプロキシ端末として選択する機能を備えたものである。

【００４３】請求項１７の発明は、請求項１４又は１５の無線端末において、基地局又は他の無線端末に対する相互認証要求に対して複数の他の無線端末又は基地局から応答を受けたとき、受信レベルの強い基地局又は他の無線端末から優先的にプロキシ端末として選択する機能を備えたものである。

【００４４】請求項１８の発明は、請求項１４又は１５の無線端末において、基地局又は他の無線端末に対する相互認証要求に対して複数の他の無線端末又は基地局か

ら応答を受けたとき、相互認証で取得した他の無線端末又は基地局の情報に基づいてプロキシ端末を選択する機能を備えたものである。

【００４５】請求項１６～１８の発明の無線端末（ＭＴ）では、ＭＴ－ＡＰ（基地局）間相互認証の際にＭＴ－ＡＳ（認証サーバ）間相互認証用パケットを中継させるＡＰ又はＭＴとして最適なものを選択する機能を備えたことで、同じ認証処理が同時に複数発生してしまうことを防止することができる。

【００４６】

【発明の実施の形態】以下、本発明の実施の形態を図に基づいて詳説する。

【００４７】［第１の実施の形態］図１は本発明の第１の実施の形態の無線アクセスネットワークの機能構成を示し、図２は認証サーバＡＳの機能構成、図３は基地局ＡＰの機能構成、図４は無線端末ＭＴの機能構成を示している。この実施の形態の無線アクセスネットワークは、無線端末ＭＴ、この無線端末ＭＴと無線通信する基地局ＡＰ、この基地局ＡＰと事業者側有線ネットワークＮＷを通じて接続される認証サーバＡＳから構成される。

【００４８】認証サーバＡＳはソフトウェアとして、無線端末ＭＴとの相互認証を実行する無線端末との認証機能１０１、認証した無線端末ＭＴを、データベースを利用して管理する無線端末管理機能１０２、ネットワークＮＷのパケットを検査する有線区間パケット検査機能１０３、パケット判別機能１０４を備え、加えて、基地局との相互認証を実行する基地局との相互認証機能１０５、認証した基地局ＡＰを、データベースを利用して管理する基地局管理機能１０６を備えている。

【００４９】基地局ＡＰはソフトウェアとして、認証サーバＡＳ－無線端末ＭＴ間の認証用パケットの転送を行う認証用パケット転送機能２０１、無線ネットワークのパケットを検査する無線区間パケット検査機能２０２、有線ネットワークＮＷのパケットを検査する有線区間パケット検査機能２０３、パケット判別機能２０４を備え、加えて、認証サーバＡＳとの相互認証を実行する認証サーバとの相互認証機能２０６、無線端末ＭＴとの相互認証を実行する無線端末との相互認証機能２０７、受信したパケットの転送可否を判断するパケット転送判断機能２０８、データベースを利用して無線端末ＭＴを管理する無線端末管理機能２０９を備えている。

【００５０】無線端末ＭＴはソフトウェアとして、認証サーバＡＳとの相互認証を実行する認証サーバとの相互認証機能３０１、無線ネットワークのパケットを検査する無線区間パケット検査機能３０２、パケット判別機能３０３を備え、加えて、基地局ＡＰとの相互認証を実行する基地局との相互認証機能３０５を備えている。

【００５１】次に、上記構成の第１の実施の形態の無線アクセスネットワークの動作について、説明する。

【００５２】＜基地局ＡＰ－認証サーバＡＳ間の相互認証＞基地局ＡＰは一般ユーザが設置し、この基地局ＡＰから事業者の認証サーバＡＳへのアクセス回線はそのユーザが契約したものとする。その基地局ＡＰは設置したユーザだけでなく、他ユーザも使用することができる。他ユーザがその基地局ＡＰを使用したとき、基地局ＡＰを設置したユーザに対して事業者からペイバックが行われる。

【００５３】ネットワークＮＷに一般ユーザが新規に基地局（ＡＰ＃ｋとする）を設置した時、この基地局ＡＰ＃ｋは事業者が管理する認証サーバＡＳと認証を行う。認証シーケンスを図５、認証用パケットペイロードデータを図６に示す。また、ＡＰ側から見た認証フローを図４に示し、ＡＳ側から見た認証フローを図８に示す。

【００５４】初めに、図４のフローのステップＳ１０１で、基地局ＡＰ＃ｋは鍵生成情報ＫＥａｐ＃ｋを計算し、その鍵生成情報を添付した認証要求を送信する。

【００５５】図８のフローのステップＳ１１１で、その認証要求を受信した認証サーバＡＳは鍵生成情報ＫＥａｓを計算し、基地局の鍵生成情報ＫＥａｐ＃ｋとこの認証サーバ側の鍵生成情報ＫＥａｓからＡＰ＃ｋ－ＡＳ間の共有鍵Ｋａｐ＃ｋ－ａｓを計算する（ステップＳ１１２）。認証サーバＡＳはさらに乱数Ｒ１を計算し、鍵生成情報ＫＥａｓと乱数Ｒ１を添付した認証要求応答をＡＰ＃ｋへ送信する（ステップＳ１１３）。

【００５６】図４のフローのステップＳ１０２で、認証要求応答を受信した基地局ＡＰ＃ｋは、ＫＥａｐ＃ｋとＫＥａｓからＡＰ＃ｋ－ＡＳ間の共有鍵Ｋａｐ＃ｋ－ａｓを計算し（ステップＳ１０３）、Ｒ１、自装置の秘密鍵ＳＫａｐ＃ｋを用いて署名データＳｉｇａｐ＃ｋを計算する（ステップＳ１０４）。基地局ＡＰ＃ｋはさらに乱数Ｒ２を計算し、Ｒ２、自装置の証明書Ｃｅｒｔａｐ＃ｋ、そしてＳｉｇａｐ＃ｋを認証情報に添付してそのパケットを認証サーバＡＳへ送信する（ステップＳ１０５）。

【００５７】図８のフローのステップＳ１１４で基地局ＡＰ＃ｋから認証情報を受信した認証サーバＡＳは、Ｃｅｒｔａｐ＃ｋを検査する（ステップＳ１１５）。もし検査が失敗した場合は、認証失敗を示す認証結果をＡＰ＃ｋへ送信する（ステップＳ１１７，Ｓ１１８）。Ｃｅｒｔａｐ＃ｋの検査が成功した場合は、さらにこのＣｅｒｔａｐ＃ｋからＡＰ＃ｋの公開鍵ＰＫａｐ＃ｋを取り出し、このＰＫａｐ＃ｋを用いてＳｉｇａｐ＃ｋを検査する（ステップＳ１１５）。もし検査が失敗した場合にも認証失敗を示す認証結果をＡＰ＃ｋへ送信する（ステップＳ１１７，Ｓ１１８）。

【００５８】ステップＳ１１５の検査が成功した場合は、認証サーバＡＳは基地局ＡＰ＃ｋが正規のものであると判断し、Ｒ２、自装置の秘密鍵ＳＫａｓを用いて署名データＳｉｇａｓを計算する（ステップＳ１１６）。

そして認証サーバＡＳは、自装置の証明書Ｃｅｒｔａｓと署名データＳｉｇａｓを認証結果に添付し、そのパケットをＡＰ＃ｋへ送信する（ステップＳ１１８）。

【００５９】図４のフローのステップＳ１０６で、認証サーバＡＳから認証結果を受信した基地局ＡＰ＃ｋは、受信したＣｅｒｔａｓを検査する。もし検査が失敗した場合は、最初から認証処理を開始する（ステップＳ１０７でＮＯに分岐）。検査が成功した場合にはさらに、ＣｅｒｔａｓからＡＳの公開鍵ＰＫａｓを取り出し、このＰＫａｓを用いてＳｉｇａｓをも検査する。ＡＰは、この検査も成功した場合は、ＡＳは事業者が設置した正規のＡＳであると判断し、ＡＰ＃ｋ－ＡＳ間の相互認証が完了する。ステップＳ１０７でＳｉｇａｓの検査が失敗した場合にも、受信した認証結果を破棄し、最初から認証処理を開始する。

【００６０】このようにして、認証サーバＡＳが新規基地局ＡＰを認証すればデータベースに登録することで、事業者はユーザが設置したＡＰを把握し、他のユーザはそうしたＡＰを事業者が設置したものと同等の安全性を持つものとみなして使用することができる。

【００６１】＜無線端末ＭＴ－基地局ＡＰ間の相互認証＞ある新規の無線端末ＭＴ＃ｉがＡＰ＃ｋを介してネットワークＮＷにアクセスしようとしたとき、ＭＴ＃ｉは初めにＡＰ＃ｋと認証を行う。ＡＰ＃ｋはこの認証が成功するまでＭＴ＃ｉから送信されたパケットを事業者側ネットワークＮＷに転送しない。ＭＴ認証シーケンスを図９に、認証用パケットのペイロードデータを図１０に示す。さらに、ＭＴ側から見た認証フローを図１１に示し、ＡＰ側から見た認証フローを図１２に示す。

【００６２】初めに、図１１のフローのステップＳ２０１で、無線端末ＭＴ＃ｉは鍵生成情報ＫＥｍｔ＃ｉを計算し、その鍵生成情報を添付した認証要求１を基地局ＡＰ＃ｋへ送信する。

【００６３】図１２のフローのステップＳ２１１で、無線端末ＭＴ＃ｉからの認証要求１を受信した基地局ＡＰ＃ｋは、鍵生成情報ＫＥａｐ＃ｋを計算し、無線端末側の鍵生成情報ＫＥｍｔ＃ｉと当該基地局側の鍵生成情報ＫＥａｐ＃ｋからＭＴ＃ｉ－ＡＰ＃ｋ間の共有鍵Ｋｍｔ＃ｉ－ａｐ＃ｋを計算する（ステップＳ２１２）。基地局ＡＰ＃ｋはさらに乱数Ｒ１を計算し、鍵生成情報ＫＥａｐ＃ｋ、乱数Ｒ１を添付した認証要求応答１を無線端末ＭＴ＃ｉへ送信する（ステップＳ２１３）。

【００６４】図１１のフローのステップＳ２０２で、基地局ＡＰ＃ｋからの認証要求応答１を受信した無線端末ＭＴ＃ｉは、自装置の鍵生成情報ＫＥｍｔ＃ｉと基地局の鍵生成情報ＫＥａｐ＃ｋからＭＴ＃ｉ－ＡＰ＃ｋ間の共有鍵Ｋｍｔ＃ｉ－ａｐ＃ｋを計算し（ステップＳ２０３）、さらに乱数Ｒ１、自装置の秘密鍵ＳＫｍｔ＃ｉを用いて署名データＳｉｇｍｔ＃ｉを計算する（ステップＳ２０４）。当該無線端末ＭＴ＃ｉはさらに、乱数Ｒ２を計算し、Ｒ２、自装置の証明書Ｃｅｒｔｍｔ＃ｉ、署名データＳｉｇｍｔ＃ｉを認証情報１に添付してそのパケットを基地局ＡＰ＃ｋへ送信する（ステップＳ２０５）。

【００６５】図１２のフローのステップＳ２１４で、無線端末ＭＴ＃ｉからの認証情報１を受信したＡＰ＃ｋは、Ｃｅｒｔｍｔ＃ｉを検査する（ステップＳ２１５）。もし検査が失敗した場合は、認証失敗を示す認証結果１をＭＴ＃ｉに送信する（ステップＳ２１９～Ｓ２２１）。検査が成功した場合はＣｅｒｔｍｔ＃ｉからＭＴ＃ｉの公開鍵ＰＫｍｔ＃ｉを取り出す。基地局ＡＰ＃ｋはＭＴ＃ｉの公開鍵ＰＫｍｔ＃ｉを用いてＳｉｇｍｔ＃ｉも検査する（ステップＳ２１５）。

【００６６】基地局ＡＰ＃ｋは、この検査が成功すれば無線端末ＭＴ＃ｉが正規のＭＴであると判断し、乱数Ｒ２、自装置の秘密鍵ＳＫａｐ＃ｋを用いて署名データＳｉｇａｐ＃ｋを計算する（ステップＳ２１６）。そして基地局ＡＰ＃ｋは、自装置の証明書Ｃｅｒｔａｐ＃ｋと署名データＳｉｇａｐ＃ｋを認証結果１に添付し、そのパケットを無線端末ＭＴ＃ｉへ送信する（ステップＳ２１７）。また基地局ＡＰ＃ｋは、無線端末ＭＴ＃ｉの認証が成功した時点で、ＭＴ＃ｉから送信される認証２用パケットの認証サーバＡＳへの転送を許可する（ステップＳ２１８）。ステップＳ２１５で無線端末ＭＴ＃ｉの署名データＳｉｇｍｔ＃ｉの検査が失敗した場合にも、認証失敗を示す認証結果１をＭＴ＃ｉに送信し（ステップＳ２１９，Ｓ２２０）、無線端末ＭＴ＃ｉから送信される認証２用パケットの認証サーバＡＳへの転送を不許可にする（ステップＳ２２１）。

【００６７】図１１のフローのステップＳ２０６で、基地局ＡＰ＃からの認証結果１を受信したＭＴ＃ｉは、基地局の証明書Ｃｅｒｔａｐ＃ｋを検査する（ステップＳ２０７）。もし検査が失敗した場合は、認証１を最初から開始する（ステップＳ２０７でＮＯに分岐）。検査が正しい場合はこのＣｅｒｔａｐ＃ｋから基地局ＡＰ＃ｋの公開鍵ＰＫａｐ＃ｋを取り出す。さらに無線端末ＭＴ＃ｉは、取り出した公開鍵ＰＫａｐ＃ｋを用いて基地局ＡＰ＃ｋの署名データＳｉｇａｐ＃ｋを検査する。この検査も正しい場合は、この基地局ＡＰ＃ｋが事業者の認めた正規のＡＰであると判断し、ＭＴ＃ｉ－ＡＰ＃ｋ間の相互認証が完了する（ステップＳ２０７でＹＥＳに分岐）。もし検査が失敗した場合にも、認証１を最初から開始する（ステップＳ２０７でＮＯに分岐）。

【００６８】このようにして、基地局ＡＰ＃ｋは無線端末ＭＴ＃ｉの認証に成功するまで事業者側ネットワークに当該無線端末ＭＴ＃ｉによるパケットを送信しないので、不正な無線端末による認証を利用した認証サーバＡＳへの攻撃を防止することができる。同時に、基地局ＡＰを所有するユーザのアクセス回線が不正に利用されることも防止することができる。

【００６９】＜無線端末ＭＴ＃ｉ－認証サーバＡＳ間の相互認証＞上記の無線端末ＭＴ＃ｉ－基地局ＡＰ＃ｋ間の相互認証が成功したら、無線端末ＭＴ＃ｉは当該基地局ＡＰ＃ｋを介して認証サーバＡＳとの認証を行う。無線端末ＭＴ＃ｉ側から見た認証フローを図１３に示し、認証サーバＡＳ側から見た認証フローを図１４に示す。さらに、基地局ＡＰ＃Ｋ側から見た認証フローを図１５、図１６に示す。そしてパケットペイロードデータは図１０に示すものである。

【００７０】図１３のフローのステップＳ２３１で、初めに、無線端末ＭＴ＃ｉはシーケンス番号ＳＱＮを生成し、そのＳＱＮと共有鍵Ｋｍｔ＃ｉ－ａｐ＃ｋを用いて送信元を示すパケット検査データＰＣＶを計算する。無線端末ＭＴ＃ｉは、これらのＳＱＮ、ＰＣＶを付加した認証要求２を基地局ＡＰ＃ｋへ送信する（ステップＳ２３２）。

【００７１】図１５のフローのステップＳ２４１で、無線端末ＭＴ＃ｉからの認証要求２を受信した基地局ＡＰ＃ｋは、ＰＣＶをＳＱＮ、Ｋｍｔ＃ｉ－ａｐ＃ｋを用いて検査する。もし検査が失敗した場合は受信した認証要求２を破棄する。検査が成功した場合は受信パケット中のＳＱＮと共有鍵Ｋａｐ＃ｋ－ａｓを用いてＰＣＶを計算する（ステップＳ２４２）。基地局ＡＰ＃ｋは、この新ＰＣＶを生成すると、元のＰＣＶを廃棄し、新しいＰＣＶを付加した認証要求２を認証サーバＡＳへ送信する（ステップＳ２４３）。

【００７２】図１４のフローのステップＳ２５１で、基地局ＡＰ＃ｋから認証要求２を受信した認証サーバＡＳは、受信したＰＣＶをシーケンス番号ＳＱＮ、共有鍵Ｋａｐ＃ｋ－ａｓを用いて検査する（ステップＳ２５２）。もし検査が失敗した場合は受信した認証要求２を破棄する。検査が成功した場合は乱数Ｒ３を計算する。認証サーバＡＳはさらに、シーケンス番号ＳＱＮを生成し、そのＳＱＮと共有鍵Ｋａｐ＃ｋ－ａｓを用いてＰＣＶを計算し（ステップＳ２５３）、乱数Ｒ３とこれらのＳＱＮ、ＰＣＶを付加した認証要求応答２を基地局ＡＰ＃ｋへ送信する（ステップＳ２５４）。

【００７３】図１５のフローのステップＳ２４１で、認証サーバＡＳから認証要求応答２を受信した基地局ＡＰ＃ｋは、シーケンス番号ＳＱＮと共有鍵Ｋａｐ＃ｋ－ａｓを用いてＰＣＶを検査する。この検査の結果が正しければ、基地局ＡＰ＃ｋはＳＱＮと共有鍵Ｋｍｔ＃ｉ－ａｐ＃ｋを用いて新しいＰＣＶを計算する（ステップＳ２４２）。基地局ＡＰ＃ｋは新しいＰＣＶを生成すると旧いＰＣＶを廃棄し、新しいＰＣＶを付加した認証要求応答２を無線端末ＭＴ＃ｉへ送信する（ステップＳ２４３）。

【００７４】図１３のフローのステップＳ２３３で、認証要求応答２を受信した無線端末ＭＴ＃ｉは、ＰＣＶをＳＱＮ、Ｋｍｔ＃ｉ－ａｐ＃ｋを用いて検査する（ステップＳ２３４）。もし検査が失敗した場合は、受信した認証要求応答２を破棄する。無線端末ＭＴ＃ｉは、ＰＣＶの検査が成功した場合は、乱数Ｒ３、秘密鍵ＳＫｍｔ＃ｉを用いて署名データＳｉｇｍｔ＃ｉを計算する（ステップＳ２３５）。さらに無線端末ＭＴ＃ｉは、乱数Ｒ４を計算し、この乱数Ｒ４、自装置の証明書Ｃｅｒｔｍｔ＃ｉ、署名データＳｉｇｍｔ＃ｉ及び上記と同様の手順で計算したＰＣＶを認証情報２に付加してそのパケットを基地局ＡＰ＃ｋへ送信する（ステップＳ２３６，Ｓ２３７）。

【００７５】図１５のフローのステップＳ２４１で、無線端末ＭＴ＃ｉからの認証情報２を受信した基地局ＡＰ＃ｋはＰＣＶを検査し、正しければ上記と同様の手順で計算したＰＣＶを付加して認証情報２を認証サーバＡＳへ送信する（ステップＳ２４２，Ｓ２４３）。

【００７６】図１４のフローのステップＳ２５５で、基地局ＡＰ＃ｋからの認証情報２を受信したＡＳは、ＰＣＶを検査する（ステップＳ２５６）。もし検査が失敗した場合は、受信した認証情報２を破棄する。検査が成功した場合は署名データＣｅｒｔｍｔ＃ｉを検査する。もし検査が失敗した場合は認証失敗を示す認証結果２に新しいＳＱＮ、上記と同様の手順で計算したＰＣＶを付加して基地局ＡＰ＃ｋへ送信する（ステップＳ２６１～Ｓ２６３）。ステップＳ２５７で署名データＣｅｒｔｍｔ＃ｉの検査が成功した場合は、この署名データＣｅｒｔｍｔ＃ｉから無線端末ＭＴ＃ｉの公開鍵ＰＫｍｔ＃ｉを取り出す。認証サーバＡＳはさらに、この公開鍵ＰＫｍｔ＃ｉを用いて署名データＳｉｇｍｔ＃ｉを検査する（ステップＳ２５７）。

【００７７】認証サーバＡＳはステップＳ２５７でＭＴ＃ｉの検査も成功すれば、無線端末ＭＴ＃ｉが正規のＭＴであると判断し、乱数Ｒ４、自装置の秘密鍵ＳＫａｓを用いて署名データＳｉｇａｓを計算する（ステップＳ２５８）。認証サーバＡＳはさらに、自装置の証明書Ｃｅｒｔａｓと Ｓｉｇａｓ、上記と同様の手順で計算したＰＣＶを認証結果２に付加し、そのパケットを基地局ＡＰ＃ｋへ送信する（ステップＳ２５９，Ｓ２６０）。この検査が失敗した場合にも、認証失敗を示す認証結果２に新しいＳＱＮ、ＰＣＶ付加して基地局ＡＰ＃ｋへ送信する（ステップＳ２６１～Ｓ２６３）。

【００７８】図１６のフローのステップＳ２７１で、認証サーバＡＳから認証結果２を受信した基地局ＡＰ＃ｋは、ＰＣＶを検査し、結果が正しければ新しいＰＣＶを付加して認証結果２をＭＴ＃ｉへ送信する（ステップＳ２７２～Ｓ２７４）。この認証結果２が認証成功を示している場合は、基地局ＡＰ＃ｋはこの時点でＭＴ＃ｉから送信されるデータパケットの事業者側ネットワークへの転送を許可する（ステップＳ２７５）。

【００７９】ステップＳ２７１で受信した認証結果２が認証失敗を示している場合、基地局ＡＰ＃ｋは無線端末

ＭＴ＃ｉから送信されるデータパケットの事業者側ネットワークへの転送を許可しない（ステップＳ２７２，Ｓ２７６～Ｓ２７８）。

【００８０】図１３のフローのステップＳ２３８で認証結果２を受信した無線端末ＭＴ＃ｉは、ＰＣＶを検査する（ステップＳ２３９）。もし検査が失敗した場合は、無線端末ＭＴ＃ｉは認証情報２を再送する（ステップＳ２３６，Ｓ２３７）。検査が成功した場合、無線端末ＭＴ＃ｉはＣｅｒｔａｓを検査する（ステップＳ２４０）。もしこの検査が失敗した場合、無線端末ＭＴ＃ｉは最初から認証２を開始する。Ｃｅｒｔａｓの検査が成功した場合、無線端末ＭＴ＃ｉはＣｅｒｔａｓから認証サーバＡＳの公開鍵ＰＫａｓを取り出し、この公開鍵ＰＫａｓを用いて署名データＳｉｇａｓを検査する。もしこの検査が失敗した場合にも、最初から認証２を開始する（ステップＳ２４０でＮＯに分岐）。この署名データＳｉｇａｓの検査も成功した場合、無線端末ＭＴ＃ｉは認証サーバＡＳが事業者の認めた正規のＡＳであると判断し、ＭＴ＃ｉ－ＡＳ間の相互認証が完了する（ステップＳ２４０）。

【００８１】このように第１の実施の形態の無線アクセスネットワークでは、認証２用パケットにパケット検査データ（ＰＣＶ）を付加することで、認証サーバＡＰは正規の無線端末ＭＴから送信されたパケットであることを確認し、認証２を利用した攻撃を防止することができる。また、認証サーバＡＳは、無線端末ＭＴから送信された認証２用パケットが正規の基地局ＡＰを経由して送信されたことを確認できる。さらに、基地局ＡＰが無線端末ＭＴを認証した後に認証サーバＡＳが無線端末ＭＴを認証することで、事業者はどの基地局ＡＰにどの無線端末ＭＴがアクセスしているかを把握でき、かつ基地局ＡＰが不正に無線端末ＭＴのアクセスを申告して事業者からペイバックを受けるような不正サービス利用や不正な課金情報の申告を防止することができる。

【００８２】［第２の実施の形態］次に、本発明の無線アクセスネットワークの第２の実施の形態について、説明する。第２の実施の形態のネットワークの特徴は、図１７に示すような状況、つまり、新規無線端末ＭＴと通信できるエリアに基地局ＡＰ＃１とＡＰ＃ｋとが存在し、これらのいずれとも認証手続きのために通信できる状況で、新規無線端末ＭＴがＭＴ－ＡＳ間相互認証用パケットを中継させる基地局として適切なもの（ここではＡＰ＃ｋ）を選択することにより、同じ認証処理が同時に複数発生してしまうことを防止する機能を備えた点にある。

【００８３】これを実現するために、無線端末ＭＴは図１８、図１９に示す機能構成を備えている。すなわち、図１に示した第１の実施の形態の機能構成に加えて、基地局選択機能３０６を備えていて、この基地局選択機能３０６が、最初に受信した基地局を中継のために基地局に選択することにより同じ認証処理が同時に複数発生してしまうことを防止する。

【００８４】次に、第２の実施の形態の無線アクセスネットワークの動作を、図２０の無線端末認証シーケンス、図２１の無線端末の基地局ＡＰ選択処理を含めたＡＰ認証フローを用いて説明する。

【００８５】ネットワークＮＷに一般ユーザが新規に基地局ＡＰ＃ｋを設置した時、ＡＰ＃ｋは事業者が管理する認証サーバＡＳと認証を行うが、この手続きは第１の実施の形態と共通であり、図５の認証シーケンス、図６の認証用パケットペイロードデータ、図７及び図８のＡＰ－ＡＳ間認証フローの通りである。

【００８６】ある無線端末ＭＴ＃ｉが基地局ＡＰを介してネットワークにアクセスしようとしたとき、ＭＴ＃１は初めにＡＰと認証を行う。基地局ＡＰはこの認証が成功するまで無線端末ＭＴ＃１から送信されたパケットを事業者側ネットワークＮＷに転送しない。ＭＴ認証シーケンスを図２０に示す。なお、第２の実施の形態で用いるＭＴ認証用パケットのペイロードデータは、第１の実施の形態と同様に図１０に示すものである。また、ＡＰ側から見たＭＴ－ＡＰ間認証フローは図１２に、ＭＴ－ＡＳ間認証フローは図１３及び図１４に、中継となる基地局ＡＰ＃ｋ側のＭＴ－ＡＳ間認証フローは図１５及び図１６にそれぞれ示した第１の実施の形態のものと同様である。ただし、第２の実施の形態の場合、ＭＴ側のＭＴ－ＡＰ間認証フローが図２１に示したものに変更される点が異なる。

【００８７】図２１に示したＭＴ側から見たＭＴ－ＡＰ間認証フローのステップＳ３０１で、ある無線端末ＭＴ＃ｉがネットワークにアクセスしようとしたとき、鍵生成情報ＫＥｍｔ＃ｉを計算し、その鍵生成情報を添付した認証要求１を基地局ＡＰへブロードキャストで送信する。

【００８８】第１の実施の形態と同様に、図１２のフローのステップＳ２１１で、無線端末ＭＴ＃１から認証要求１を受信したＡＰ＃ｋは、鍵生成情報ＫＥａｐ＃ｋを計算し、さらにＭＴ＃ｉ－ＡＰ＃ｋ間の共有鍵Ｋｍｔ＃ｉ－ａｐ＃ｋを計算する（ステップＳ２１２）。さらに基地局ＡＰ＃ｋは、乱数Ｒ１を計算し、ＫＥａｐ＃ｋ、Ｒ１を添付した認証要求応答１をＭＴ＃ｉへ送信する（ステップＳ２１３）。

【００８９】図１７に示した状況では基地局ＡＰ＃１も同じ無線端末ＭＴ＃ｉからの認証要求１を受信するので、同様にして鍵生成情報ＫＥａｐ＃１を計算し、ＭＴ＃ｉ－ＡＰ＃１間の共有鍵Ｋｍｔ＃ｉ－ａｐ＃１を計算する（ステップＳ２１２）。基地局ＡＰ＃１はさらに、乱数Ｒ１’を計算し、ＫＥａｐ＃１、Ｒ１’を添付した認証要求応答１をＭＴ＃ｉへ基地局ＡＰ＃ｋと同様に送信する（ステップＳ２１３）。

【００９０】図２１のフローのステップＳ３０２～Ｓ３

０４で、無線端末ＭＴ＃ｉは予め基地局選択機能３０６に組み込まれたロジック、つまり、最初に受信した認証要求応答１に対して処理を行うというロジックに基づき、２番目以降に受信した認証処理応答１はそれよりも先に受信された基地局の認証処理応答１が選択された場合に廃棄する。ここでは、最初に基地局ＡＰ＃ｋからの認証処理応答１を受信し、基地局ＡＰ＃１からの認証処理応答１はそれに遅れて受信したものとする。

【００９１】基地局ＡＰ＃ｋからの認証要求応答１を最初に受信したＭＴ＃ｉは、ステップＳ３０５で、第１の実施の形態と同様に自装置の鍵生成情報ＫＥｍｔ＃ｉと基地局ＡＰ＃ｋの鍵生成情報ＫＥａｐ＃ｋからＭＴ＃ｉ－ＡＰ＃ｋ間の共有鍵Ｋｍｔ＃ｉ－ａｐ＃ｋを計算する。そして、乱数Ｒ１、自装置の秘密鍵ＳＫｍｔ＃ｉを用いて署名データＳｉｇｍｔ＃ｉを計算する（ステップＳ３０６）。続いて、無線端末ＭＴ＃ｉは乱数Ｒ２を計算し、Ｒ２、自装置の証明書Ｃｅｒｔｍｔ＃ｉ、Ｓｉｇｍｔ＃ｉを認証情報１に添付してそのパケットを選択した基地局ＡＰ＃ｋへ送信する（ステップＳ３０７）。

【００９２】図１２のフローのステップＳ２１４で、無線端末ＭＴ＃ｉからの認証情報１を受信した基地局ＡＰ＃ｋは、以降、第１の実施の形態と同様の処理を実行し、基地局ＭＴ＃ｉが正規のＭＴであると判断すれば、認証結果１をＭＴ＃ｉへ送信し（ステップＳ２１５～Ｓ２１７）、またＭＴ＃ｉの認証が成功した時点でＭＴ＃ｉから送信される認証２用パケットのＡＳへの転送を許可する（ステップＳ２１８）。一方、もしＭＴの検査に失敗した場合は、認証失敗を示す認証結果１をＭＴ＃ｉへ送信し、ＭＴ＃ｉから送信される認証２用パケットのＡＳへの転送を不許可にする（ステップＳ２１９～Ｓ２２１）。

【００９３】図２１のフローのステップＳ３０８で基地局ＡＰ＃ｋから認証結果１を受信した無線端末ＭＴ＃ｉは基地局ＡＰ＃ｋの証明書Ｃｅｒｔａｐ＃ｋを検査する（ステップＳ３０９）。この検査が失敗した場合は、最初から認証１を開始する。そしてこの場合、最初に受信した基地局ＡＰ＃ｋからの認証要求応答１のパケットを廃棄し、２番目に受信した基地局ＡＰ＃１からの認証要求応答１に対して認証処理を行うことになる。つまり、２度目の認証でも最初にＡＰ＃ｋ、２番目のＡＰ＃１からの応答を受信したとすれば、ステップＳ３０３，Ｓ３１１で最初のＡＰ＃ｋのパケットは破棄する。そしてステップＳ３０４で２番目に受信したＡＰ＃１の認証要求応答１について、認証処理を実施するのである。

【００９４】ステップＳ３０９において、基地局ＡＰ＃ｋの証明書Ｃｅｒｔａｐ＃ｋの検査が成功した場合は、無線端末ＭＴ＃ｉはＣｅｒｔａｐ＃ｋから基地局ＡＰ＃ｋの公開鍵ＰＫａｐ＃ｋを取り出し、このＰＫａｐ＃ｋを用いてＳｉｇａｐ＃ｋを検査し、この検査も成功すれば基地局ＡＰ＃ｋが事業者の設置した正規のＡＰであると判断し、ＭＴ＃ｉ－ＡＰ＃ｋ間の相互認証が完了する。この検査が失敗した場合にも、最初から認証１を開始する。そしてこの場合にも、２番目に受信した基地局ＡＰ＃１からの認証要求応答１に対して同様に認証処理を行うことになる。

【００９５】上記の認証１が成功したら、無線端末ＭＴ＃ｉは選択した基地局ＡＰ＃ｋを介して認証サーバＡＳと認証を行う。このＭＴ－ＡＳ間の認証手続きは、第１の実施の形態と同様であり、ＭＴ側のＭＴ－ＡＳ間認証フローは図１３に、ＡＰ側のＭＴ－ＡＳ間認証フローは図１４に、中継となる基地局ＡＰ＃ｋ側のＭＴ－ＡＳ間認証フローは図１５及び図１６にそれぞれ示したものである。

【００９６】この第２の実施の形態の無線アクセスネットワークによれば、第１の実施の形態と同様、基地局ＡＰ＃ｋが無線端末ＭＴ＃ｉの認証が成功するまで事業者側ネットワークにＭＴ＃ｉによるパケットを送信しないので、不正な無線端末による認証を利用した認証サーバＡＳへの攻撃を防止することができ、また、基地局ＡＰを所有するユーザのアクセス回線が不正に利用されることも防止することができる。さらに第２の実施の形態の場合、正規の基地局ＡＰを１つ選択することで同一の認証２用パケットが認証サーバＡＳへ同時的に送信されることを防止できる。

【００９７】［第３の実施の形態］次に、本発明の第３の実施の形態の無線アクセスネットワークについて、説明する。第３の実施の形態の無線アクセスネットワークは、機能構成は第２の実施の形態と同様であるが、図１７に示した状況、つまり、新規無線端末ＭＴ＃ｉが複数の基地局ＡＰ＃１，ＡＰ＃ｋから同時に、あるいは相前後して認証要求応答１を受信した場合に、受信信号レベルが最も高い基地局（ここではＡＰ＃ｋとする）を選択し、以降の認証手続きを実行する点に特徴を有する。図２２は、第３の実施の形態において、無線端末ＭＴの基地局選択処理を含むＡＰ認証フローを示している。その他の処理は全て第２の実施の形態と共通である。

【００９８】無線端末ＭＴの備える機能構成は、図１８に示す第２の実施の形態と同様である。ただし、基地局選択機能３０６が、受信レベルが最大である基地局を選ぶことによって同じ認証処理が同時に複数発生してしまうことを防止する点で第２の実施の形態とは異なる。

【００９９】次に、第３の実施の形態の無線アクセスネットワークの動作を、図２０の無線端末認証シーケンス、図２２の無線端末の基地局ＡＰ選択処理を含めたＡＰ認証フローを用いて説明する。

【０１００】ネットワークに一般ユーザが新規に基地局ＡＰ＃ｋを設置した時、ＡＰ＃ｋは事業者が管理する認証サーバＡＳと認証を行うが、この手続きは第１、第２の実施の形態と共通であり、図５の認証シーケンス、図６の認証用パケットペイロードデータ、図７及び図８の

ＡＰ－ＡＳ間認証フローの通りである。

【０１０１】ある無線端末ＭＴ＃ｉが基地局ＡＰを介してネットワークにアクセスしようとしたとき、ＭＴ＃１は初めにＡＰと認証を行う。基地局ＡＰはこの認証が成功するまで無線端末ＭＴ＃１から送信されたパケットを事業者側ネットワークＮＷに転送しない。なお、第３の実施の形態で用いるＭＴ認証用パケットのペイロードデータは、第１の実施の形態と同様に図１０に示すものである。また、ＡＰ側から見たＭＴ－ＡＰ間認証フローは図１２に、ＭＴ－ＡＳ間認証フローは図１３及び図１４に、中継となる基地局ＡＰ＃ｋ側のＭＴ－ＡＳ間認証フローは図１５及び図１６にそれぞれ示した第１、第２の実施の形態のものと同様である。

【０１０２】図２２に示したＭＴ側から見たＭＴ－ＡＰ間認証フローのステップＳ３０１で、ある無線端末ＭＴ＃ｉがネットワークにアクセスしようとしたとき、鍵生成情報ＫＥｍｔ＃ｉを計算し、その鍵生成情報を添付した認証要求１を基地局ＡＰへブロードキャストで送信する。

【０１０３】第１の実施の形態と同様に、図１２のフローのステップＳ２１１で、無線端末ＭＴ＃１から認証要求１を受信したＡＰ＃ｋは、鍵生成情報ＫＥａｐ＃ｋを計算し、さらにＭＴ＃ｉ－ＡＰ＃ｋ間の共有鍵Ｋｍｔ＃ｉ－ａｐ＃ｋを計算する（ステップＳ２１２）。さらに基地局ＡＰ＃ｋは、乱数Ｒ１を計算し、ＫＥａｐ＃ｋ、Ｒ３を添付した認証要求応答１をＭＴ＃ｉへ送信する（ステップＳ２１３）。

【０１０４】図１７に示した状況では基地局ＡＰ＃１も同じ無線端末ＭＴ＃ｉからの認証要求１を受信するので、同様にして鍵生成情報ＫＥａｐ＃１を計算し、ＭＴ＃ｉ－ＡＰ＃１間の共有鍵Ｋｍｔ＃ｉ－ａｐ＃１を計算する（ステップＳ２１２）。基地局ＡＰ＃１はさらに、乱数Ｒ１’を計算し、ＫＥａｐ＃１、Ｒ１’を添付した認証要求応答１をＭＴ＃ｉへ基地局ＡＰ＃ｋと同様に送信する（ステップＳ２１３）。

【０１０５】図２２のフローのステップＳ３０２～３０４′で、無線端末ＭＴ＃ｉは予め基地局選択機能３０６に組み込まれたロジック、つまり、送信後の所定時間内に受信した認証要求応答１の信号レベルが一番高い基地局を選択するというロジックに基づき基地局を選択し、それ以外の認証処理応答１は廃棄する（ステップＳ３０４′，Ｓ３１２）。したがって、最初の認証処理応答で、基地局ＡＰ＃１とＡＰ＃ｋとから所定時間内に認証要求応答１を受信した無線端末ＭＴ＃ｉは、それらの認証要求応答１の受信レベルを測定し、測定レベルの高い基地局ＡＰ＃ｋからの認証要求応答１に対して処理を行い、ＡＰ＃１の認証要求応答１のパケットは廃棄することになる。

【０１０６】図２２のフローのステップＳ３０４′で基地局ＡＰ＃ｋからの認証要求応答１を選択したＭＴ＃ｉは、ステップＳ３０５で、第１、第２の実施の形態と同様に、自装置の鍵生成情報ＫＥｍｔ＃ｉと基地局ＡＰ＃ｋの鍵生成情報ＫＥａｐ＃ｋからＭＴ＃ｉ－ＡＰ＃ｋ間の共有鍵Ｋｍｔ＃ｉ－ａｐ＃ｋを計算する。そして、乱数Ｒ１、自装置の秘密鍵ＳＫｍｔ＃ｉを用いて署名データＳｉｇｍｔ＃ｉを計算する（ステップＳ３０６）。続いて、無線端末ＭＴ＃ｉは乱数Ｒ２を計算し、Ｒ２、自装置の証明書Ｃｅｒｔｍｔ＃ｉ、Ｓｉｇｍｔ＃ｉを認証情報１に添付してそのパケットを選択した基地局ＡＰ＃ｋへ送信する（ステップＳ３０７）。

【０１０７】図１２のフローのステップＳ２１４で、無線端末ＭＴ＃ｉからの認証情報１を受信した基地局ＡＰ＃ｋは、以降、第１、第２の実施の形態と同様の処理を実行し、基地局ＭＴ＃ｉが正規のＭＴであると判断すれば、認証結果１をＭＴ＃ｉへ送信し（ステップＳ２１５～Ｓ２１７）、またＭＴ＃ｉの認証が成功した時点でＭＴ＃ｉから送信される認証２用パケットのＡＳへの転送を許可する（ステップＳ２１８）。一方、もしＭＴの検査に失敗した場合は、認証失敗を示す認証結果１をＭＴ＃ｉへ送信し、ＭＴ＃ｉから送信される認証２用パケットのＡＳへの転送を不許可にする（ステップＳ２１９～Ｓ２２１）。

【０１０８】図２２のフローのステップＳ３０８で基地局ＡＰ＃ｋから認証結果１を受信した無線端末ＭＴ＃ｉは、基地局ＡＰ＃ｋの証明書Ｃｅｒｔａｐ＃ｋを検査する（ステップＳ３０９）。この検査が失敗した場合は、ステップＳ３０１に戻り、最初から認証１を開始する。

【０１０９】ステップＳ３０９において、基地局ＡＰ＃ｋの証明書Ｃｅｒｔａｐ＃ｋの検査が成功した場合は、無線端末ＭＴ＃ｉはＣｅｒｔａｐ＃ｋから基地局ＡＰ＃ｋの公開鍵ＰＫａｐ＃ｋを取り出し、このＰＫａｐ＃ｋを用いてＳｉｇａｐ＃ｋを検査し、この検査も成功すれば基地局ＡＰ＃ｋが事業者の認めた正規のＡＰであると判断し、ＭＴ＃ｉ－ＡＰ＃ｋ間の相互認証が完了する。この検査が失敗した場合にも、最初から認証１を開始する。

【０１１０】ステップＳ３０９で最初から認証１を繰り返す判定に至った場合、無線端末ＭＴ＃ｉはブロードキャストで認証要求１を再度送信する（ステップＳ３０１）。これに対して、第１回目と同様に基地局ＡＰ＃ｋ，ＡＰ＃１が認証要求応答１を返信してきたとし、しかも基地局ＡＰ＃ｋの受信レベルの方が基地局ＡＰ＃１の受信レベルよりも高かったとする。

【０１１１】この場合、ステップＳ３０２でＭＴ＃ｉは基地局ＡＰ＃ｋを最初に選択するが、これに対してステップＳ３０３で、第１回目の判定でＮＧと判断された基地局であると判定してそのパケットを破棄する（ステップＳ３０３，Ｓ３１１）。そして次の基地局ＡＰ＃１の認証要求応答１を採用し、ステップＳ３０４′で他に受信レベルがＡＰ＃１よりも高いものがないと判定すれ

ば、この基地局ＡＰ＃１の認証要求応答１に対してステップＳ３０５以降の処理を実施する。なお、ステップＳ３０５以降の処理は、図２１のフローに示した第２の実施の形態と同様である。

【０１１２】この第３の実施の形態の無線アクセスネットワークによれば、第２の実施の形態と同様、基地局ＡＰ＃ｋが無線端末ＭＴ＃ｉの認証が成功するまで事業者側ネットワークにＭＴ＃ｉによるパケットを送信しないので、不正な無線端末による認証を利用した認証サーバＡＳへの攻撃を防止することができ、また、基地局ＡＰを所有するユーザのアクセス回線が不正に利用されることも防止することができる。さらに第３の実施の形態の場合、正規の基地局ＡＰを１つ選択することで同一の認証２用パケットが認証サーバＡＳへ送信されることを防止できる。加えて、信号受信レベルの高い基地局を選択することで無線通信の信頼性を高めることができる。

【０１１３】［第４の実施の形態］第４の実施の形態の無線アクセスネットワークは、機能構成は第２の実施の形態と同様であるが、図１７に示した状況、つまり、新規無線端末ＭＴ＃ｉが複数の基地局ＡＰ＃１，ＡＰ＃ｋから同時に、あるいは相前後して認証要求応答１を受信した場合に、受信信号レベルが最も高い基地局（ここではＡＰ＃ｋとする）を選択し、以降の認証手続きを実行する点に特徴を有する。図２３は、第４の実施の形態において、無線端末ＭＴの基地局選択処理を含むＡＰ認証フローを示している。その他の処理は全て第２、第３の実施の形態と共通である。

【０１１４】無線端末ＭＴの備える機能構成は、図１８に示す第２、第３の実施の形態と同様である。ただし、基地局選択機能３０６が、帯域使用状況を受信した複数の基地局それぞれについて確認し、最も帯域に空きがある基地局から優先的に選択して認証要求応答１に対して処理を行うことによって、同じ認証処理が同時に複数発生してしまうことを防止する点で第２、第３の実施の形態とは異なる。

【０１１５】次に、第４の実施の形態の無線アクセスネットワークの動作を、図２０の無線端末認証シーケンス、図２３の無線端末の基地局ＡＰ選択処理を含めたＡＰ認証フローを用いて説明する。

【０１１６】ネットワークに一般ユーザが新規に基地局ＡＰ＃ｋを設置した時、ＡＰ＃ｋは事業者が管理する認証サーバＡＳと認証を行うが、この手続きは第１、第２の実施の形態と共通であり、図５の認証シーケンス、図６の認証用パケットペイロードデータ、図７及び図８のＡＰ－ＡＳ間認証フローの通りである。

【０１１７】ある無線端末ＭＴ＃ｉが基地局ＡＰを介してネットワークにアクセスしようとしたとき、ＭＴ＃１は初めにＡＰと認証を行う。基地局ＡＰはこの認証が成功するまで無線端末ＭＴ＃１から送信されたパケットを事業者側ネットワークＮＷに転送しない。なお、第４の実施の形態で用いるＭＴ認証用パケットのペイロードデータも、第１の実施の形態と同様に図１０に示すものである。また、ＡＰ側から見たＭＴ－ＡＰ間認証フローは図１２に、ＭＴ－ＡＳ間認証フローは図１３及び図１４に、中継となる基地局ＡＰ＃ｋ側のＭＴ－ＡＳ間認証フローは図１５及び図１６にそれぞれ示した第１、第２の実施の形態のものと同様である。

【０１１８】図２３に示したＭＴ側から見たＭＴ－ＡＰ間認証フローのステップＳ３０１で、ある無線端末ＭＴ＃ｉがネットワークにアクセスしようとしたとき、鍵生成情報ＫＥｍｔ＃ｉを計算し、その鍵生成情報を添付した認証要求１を基地局ＡＰへブロードキャストで送信する。

【０１１９】第１の実施の形態と同様に、図１２のフローのステップＳ２１１で、無線端末ＭＴ＃１から認証要求１を受信したＡＰ＃ｋは、鍵生成情報ＫＥａｐ＃ｋを計算し、さらにＭＴ＃ｉ－ＡＰ＃ｋ間の共有鍵Ｋｍｔ＃ｉ－ａｐ＃ｋを計算する（ステップＳ２１２）。さらに基地局ＡＰ＃ｋは、乱数Ｒ１を計算し、ＫＥａｐ＃ｋ、Ｒ３を添付した認証要求応答１をＭＴ＃ｉへ送信する（ステップＳ２１３）。

【０１２０】図１７に示した状況では基地局ＡＰ＃１も同じ無線端末ＭＴ＃ｉからの認証要求１を受信するので、同様にして鍵生成情報ＫＥａｐ＃１を計算し、ＭＴ＃ｉ－ＡＰ＃１間の共有鍵Ｋｍｔ＃ｉ－ａｐ＃１を計算する（ステップＳ２１２）。基地局ＡＰ＃１はさらに、乱数Ｒ１’を計算し、ＫＥａｐ＃１、Ｒ１’を添付した認証要求応答１をＭＴ＃ｉへ基地局ＡＰ＃ｋと同様に送信する（ステップＳ２１３）。

【０１２１】図２３のフローのステップＳ３０２～３０４″で、無線端末ＭＴ＃ｉは予め基地局選択機能３０６に組み込まれたロジック、つまり、送信後の所定時間内に送信してきた基地局の中で最も帯域に空きがある基地局を選択するというロジックに基づき基地局を選択し、それ以外の認証処理応答１は廃棄する（ステップＳ３０４″，Ｓ３１２）。したがって、最初の認証処理応答で、基地局ＡＰ＃１とＡＰ＃ｋとから所定時間内に認証要求応答１を受信した無線端末ＭＴ＃ｉは、それらの基地局の帯域の空き状況を確認し、帯域の空きが大きい基地局ＡＰ＃ｋからの認証要求応答１に対して処理を行い、ＡＰ＃１の認証要求応答１のパケットは廃棄することになる。

【０１２２】図２３のフローのステップＳ３０４″で基地局ＡＰ＃ｋからの認証要求応答１を選択したＭＴ＃ｉは、ステップＳ３０５で、第１、第２の実施の形態と同様に、自装置の鍵生成情報ＫＥｍｔ＃ｉと基地局ＡＰ＃ｋの鍵生成情報ＫＥａｐ＃ｋからＭＴ＃ｉ－ＡＰ＃ｋ間の共有鍵Ｋｍｔ＃ｉ－ａｐ＃ｋを計算する。そして、乱数Ｒ１、自装置の秘密鍵ＳＫｍｔ＃ｉを用いて署名データＳｉｇｍｔ＃ｉを計算する（ステップＳ３０６）。続

いて、無線端末ＭＴ＃ｉは乱数Ｒ２を計算し、Ｒ２、自装置の証明書Ｃｅｒｔｍｔ＃ｉ、Ｓｉｇｍｔ＃ｉを認証情報１に添付してそのパケットを選択した基地局ＡＰ＃ｋへ送信する（ステップＳ３０７）。

【０１２３】図１２のフローのステップＳ２１４で、無線端末ＭＴ＃ｉからの認証情報１を受信した基地局ＡＰ＃ｋは、以降、第１、第２の実施の形態と同様の処理を実行し、基地局ＭＴ＃ｉが正規のＭＴであると判断すれば、認証結果１をＭＴ＃ｉへ送信し（ステップＳ２１５～Ｓ２１７）、またＭＴ＃ｉの認証が成功した時点でＭＴ＃ｉから送信される認証２用パケットのＡＳへの転送を許可する（ステップＳ２１８）。一方、もしＭＴの検査に失敗した場合は、認証失敗を示す認証結果１をＭＴ＃ｉへ送信し、ＭＴ＃ｉから送信される認証２用パケットのＡＳへの転送を不許可にする（ステップＳ２１９～Ｓ２２１）。

【０１２４】図２３のフローのステップＳ３０８で基地局ＡＰ＃ｋから認証結果１を受信した無線端末ＭＴ＃ｉは、基地局ＡＰ＃ｋの証明書Ｃｅｒｔａｐ＃ｋを検査する（ステップＳ３０９）。この検査が失敗した場合は、ステップＳ３０１に戻り、最初から認証１を開始する。

【０１２５】ステップＳ３０９において、基地局ＡＰ＃ｋの証明書Ｃｅｒｔａｐ＃ｋの検査が成功した場合は、無線端末ＭＴ＃ｉはＣｅｒｔａｐ＃ｋから基地局ＡＰ＃ｋの公開鍵ＰＫａｐ＃ｋを取り出し、このＰＫａｐ＃ｋを用いてＳｉｇａｐ＃ｋを検査し、この検査も成功すれば基地局ＡＰ＃ｋが事業者の認めた正規のＡＰであると判断し、ＭＴ＃ｉ－ＡＰ＃ｋ間の相互認証が完了する。この検査が失敗した場合にも、最初から認証１を開始する。

【０１２６】ステップＳ３０９で最初から認証１を繰り返す判定に至った場合、無線端末ＭＴ＃ｉはブロードキャストで認証要求１を再度送信する（ステップＳ３０１）。これに対して、第１回目と同様に基地局ＡＰ＃ｋ，ＡＰ＃１が認証要求応答１を返信してきたとし、しかも第２回目にも基地局ＡＰ＃ｋの方がａｐ＃１よりも使用帯域の空きが大きかったとする。

【０１２７】この場合、ステップＳ３０２でＭＴ＃ｉは基地局ＡＰ＃ｋを最初に選択するが、これに対してステップＳ３０３で、第１回目の判定でＮＧと判断された基地局であると判定してそのパケットを破棄する（ステップＳ３０３，Ｓ３１１）。そして次の基地局ＡＰ＃１の認証要求応答１を採用し、ステップＳ３０４″で他に候補となる基地局がないと判定すれば、この基地局ＡＰ＃１の認証要求応答１に対してステップＳ３０５以降の処理を実施する。なお、ステップＳ３０５以降の処理は、図２１のフローに示した第２の実施の形態の処理と同様である。

【０１２８】この第４の実施の形態の無線アクセスネットワークによれば、第２の実施の形態と同様、基地局ＡＰ＃ｋが無線端末ＭＴ＃ｉの認証が成功するまで事業者側ネットワークにＭＴ＃ｉによるパケットを送信しないので、不正な無線端末による認証を利用した認証サーバＡＳへの攻撃を防止することができ、また、基地局ＡＰを所有するユーザのアクセス回線が不正に利用されることも防止することができる。さらに第４の実施の形態の場合、正規の基地局ＡＰを１つ選択することで同一の認証２用パケットが認証サーバＡＳへ送信されることを防止できる。加えて、使用帯域の空きが大きい基地局を選択することで無線通信の応答速度を高めることができる。

【０１２９】［第５の実施の形態］次に、本発明の第５の実施の形態の無線アクセスネットワークについて、説明する。第５の実施の形態の無線アクセスネットワークは、機能構成は第２の実施の形態と同様であるが、図１７に示した状況、つまり、新規無線端末ＭＴ＃ｉが複数の基地局ＡＰ＃１，ＡＰ＃ｋから同時に、あるいは相前後して認証要求応答１を受信した場合に、そのすべてを一旦保持しておき、応答が早い基地局から順に認証１の処理を実施し、認証１が成功した基地局を選択し、以降の認証手続きを実行する点に特徴を有する。図２４は、第５の実施の形態において、無線端末ＭＴの基地局選択処理を含むＡＰ認証フローを示している。その他の処理は全て第２の実施の形態と共通である。

【０１３０】無線端末ＭＴの備える機能構成は、図１８に示す第２の実施の形態と同様である。ただし、基地局選択機能３０６が、複数の基地局から認証要求応答１を受信した場合に、そのすべてを一旦保持しておき、応答が早い基地局から順に認証１の処理を実施し、認証１が成功した基地局を選択することにより同じ認証処理が同時に複数発生してしまうことを防止する点で第２の実施の形態とは異なる。

【０１３１】次に、第５の実施の形態の無線アクセスネットワークの動作を、図２０の無線端末認証シーケンス、図２４の無線端末の基地局ＡＰ選択処理を含めたＡＰ認証フローを用いて説明する。

【０１３２】ネットワークに一般ユーザが新規に基地局ＡＰ＃ｋを設置した時、ＡＰ＃ｋは事業者が管理する認証サーバＡＳと認証を行うが、この手続きは第１、第２の実施の形態と共通であり、図５の認証シーケンス、図６の認証用パケットペイロードデータ、図７及び図８のＡＰ－ＡＳ間認証フローの通りである。

【０１３３】ある無線端末ＭＴ＃ｉが基地局ＡＰを介してネットワークにアクセスしようとしたとき、ＭＴ＃１は初めにＡＰと認証を行う。基地局ＡＰはこの認証が成功するまで無線端末ＭＴ＃１から送信されたパケットを事業者側ネットワークＮＷに転送しない。なお、第５の実施の形態で用いるＭＴ認証用パケットのペイロードデータは、第１の実施の形態と同様に図１０に示すものである。また、ＡＰ側から見たＭＴ－ＡＰ間認証フローは

図１２に、ＭＴ－ＡＳ間認証フローは図１３及び図１４に、中継となる基地局ＡＰ＃ｋ側のＭＴ－ＡＳ間認証フローは図１５及び図１６にそれぞれ示した第１、第２の実施の形態のものと同様である。

【０１３４】図２４に示したＭＴ側から見たＭＴ－ＡＰ間認証フローのステップＳ４０１で、ある無線端末ＭＴ＃ｉがネットワークにアクセスしようとしたとき、鍵生成情報ＫＥｍｔ＃ｉを計算し、その鍵生成情報を添付した認証要求１を基地局ＡＰへブロードキャストで送信する。

【０１３５】第１の実施の形態と同様に、図１２のフローのステップＳ２１１で、無線端末ＭＴ＃１から認証要求１を受信したＡＰ＃ｋは、鍵生成情報ＫＥａｐ＃ｋを計算し、さらにＭＴ＃ｉ－ＡＰ＃ｋ間の共有鍵Ｋｍｔ＃ｉ－ａｐ＃ｋを計算する（ステップＳ２１２）。さらに基地局ＡＰ＃ｋは、乱数Ｒ１を計算し、ＫＥａｐ＃ｋ、Ｒ１を添付した認証要求応答１をＭＴ＃ｉへ送信する（ステップＳ２１３）。

【０１３６】図１７に示した状況では基地局ＡＰ＃１も同じ無線端末ＭＴ＃ｉからの認証要求１を受信するので、同様にして鍵生成情報ＫＥａｐ＃１を計算し、ＭＴ＃ｉ－ＡＰ＃１間の共有鍵Ｋｍｔ＃ｉ－ａｐ＃１を計算する（ステップＳ２１２）。基地局ＡＰ＃１はさらに、乱数Ｒ１’を計算し、ＫＥａｐ＃１、Ｒ１’を添付した認証要求応答１をＭＴ＃ｉへ基地局ＡＰ＃ｋと同様に送信する（ステップＳ２１３）。

【０１３７】図２４のフローのステップＳ４０２，Ｓ４０３で、無線端末ＭＴ＃ｉは予め基地局選択機能３０６に組み込まれたロジック、つまり、送信後の所定時間内に受信した認証要求応答１のうち最先に受信した基地局を選択するというロジックに基づき基地局を選択し、それ以外の認証処理応答１に対する認証処理は保留にする。ここでは、基地局ＡＰ＃ｋからの認証処理応答１が最先であったとして説明する。

【０１３８】基地局ＡＰ＃１とＡＰ＃ｋとから所定時間内に認証要求応答１を受信した無線端末ＭＴ＃ｉは、最先に応答してきた基地局ＡＰ＃ｋからの認証要求応答１に対して処理を行う（ステップＳ４０２～Ｓ４０４）。他の受信した基地局ＡＰ＃１からの認証処理応答１は、それよりも先に応答した基地局について認証１が成功するまでは保持されるが、先に応答した基地局が選択された時点で廃棄することになる。

【０１３９】図２４のフローのステップＳ４０４で基地局ＡＰ＃ｋからの認証要求応答１を選択したＭＴ＃ｉは、ステップＳ４０５で、第１、第２の実施の形態と同様に、自装置の鍵生成情報ＫＥｍｔ＃ｉと基地局ＡＰ＃ｋの鍵生成情報ＫＥａｐ＃ｋからＭＴ＃ｉ－ＡＰ＃ｋ間の共有鍵Ｋｍｔ＃ｉ－ａｐ＃ｋを計算する。そして、乱数Ｒ１、自装置の秘密鍵ＳＫｍｔ＃ｉを用いて署名データＳｉｇｍｔ＃ｉを計算する（ステップＳ４０６）。続いて、無線端末ＭＴ＃ｉは乱数Ｒ２を計算し、Ｒ２、自装置の証明書Ｃｅｒｔｍｔ＃ｉ、Ｓｉｇｍｔ＃ｉを認証情報１に添付してそのパケットを選択した基地局ＡＰ＃ｋへ送信する（ステップＳ４０７）。

【０１４０】図１２のフローのステップＳ２１４で、無線端末ＭＴ＃ｉからの認証情報１を受信した基地局ＡＰ＃ｋは、以降、第１、第２の実施の形態と同様の処理を実行し、基地局ＭＴ＃ｉが正規のＭＴであると判断すれば、認証結果１をＭＴ＃ｉへ送信し（ステップＳ２１５～Ｓ２１７）、またＭＴ＃ｉの認証が成功した時点でＭＴ＃ｉから送信される認証２用パケットのＡＳへの転送を許可する（ステップＳ２１８）。一方、もしＭＴの検査に失敗した場合は、認証失敗を示す認証結果１をＭＴ＃ｉへ送信し、ＭＴ＃ｉから送信される認証２用パケットのＡＳへの転送を不許可にする（ステップＳ２１９～Ｓ２２１）。

【０１４１】図２４のフローのステップＳ４０８で基地局ＡＰ＃ｋから認証結果１を受信した無線端末ＭＴ＃ｉは基地局ＡＰ＃ｋの証明書Ｃｅｒｔａｐ＃ｋを検査する（ステップＳ４０９）。この検査が失敗した場合は、当該パケットを破棄し（ステップＳ４１１）、他の基地局からの認証要求応答１を受信しているかどうか判断する（ステップＳ４１２）。

【０１４２】ステップＳ４１２で、他の基地局からの認証要求応答１が残っている場合にはステップＳ４０４に戻り、残っている認証要求応答１のうち応答が最も早かった基地局を選択し、ステップＳ４０５以降の処理を繰り返す。図１７の状況では、最初に基地局ＡＰ＃１が選択されることになるが、基地局ＡＰ＃ｋの認証が不成功であれば、続いて応答してきた基地局ＡＰ＃１について、ステップＳ４０５以降の処理が実施されることになる。なお、ステップＳ４１２において、他の基地局からの認証要求応答１が残っていない場合には、ステップＳ４０１に戻り、最初から認証１を開始する。

【０１４３】ステップＳ４０９において、基地局ＡＰ＃ｋの証明書Ｃｅｒｔａｐ＃ｋの検査が成功した場合は、無線端末ＭＴ＃ｉはＣｅｒｔａｐ＃ｋから基地局ＡＰ＃ｋの公開鍵ＰＫａｐ＃ｋを取り出し、このＰＫａｐ＃ｋを用いてＳｉｇａｐ＃ｋを検査し、この検査も成功すれば基地局ＡＰ＃ｋが事業者の認めた正規のＡＰであると判断し、ＭＴ＃ｉ－ＡＰ＃ｋ間の相互認証が完了する。この検査が失敗した場合にも、ステップＳ４１１，Ｓ４１２を実行し、２番目に応答してきた基地局ＡＰ＃１からの認証要求応答１に対して同様に認証処理を行う。

【０１４４】上記の認証１が成功したら、無線端末ＭＴ＃ｉは選択した基地局ＡＰ＃ｋを介して認証サーバＡＳと認証を行う。このＭＴ－ＡＳ間の認証手続きは、第１、第２の実施の形態と同様であり、ＭＴ側のＭＴ－ＡＳ間認証フローは図１３に、ＡＰ側のＭＴ－ＡＳ間認証フローは図１４に、中継となる基地局ＡＰ＃ｋ側のＭＴ

－ＡＳ間認証フローは図１５及び図１６にそれぞれ示したものである。

【０１４５】この第５の実施の形態の無線アクセスネットワークによれば、第１の実施の形態と同様、基地局ＡＰ＃ｋが無線端末ＭＴ＃ｉの認証が成功するまで事業者側ネットワークにＭＴ＃ｉによるパケットを送信しないので、不正な無線端末による認証を利用した認証サーバＡＳへの攻撃を防止することができ、また、基地局ＡＰを所有するユーザのアクセス回線が不正に利用されることも防止することができる。さらに第５の実施の形態の場合、正規の基地局ＡＰを１つ選択することで同一の認証２用パケットが認証サーバＡＳへ送信されることを防止できる。加えて、最先に応答した基地局から優先的に選択することで無線通信の応答速度を速めることができ、複数の基地局からの応答を無線端末側で一旦保持しておいて応答の時間的に早かったものから優先して認証処理を実施するので、第３の実施の形態の場合よりも通信処理が迅速化できる。

【０１４６】［第６の実施の形態］次に、本発明の第６の実施の形態の無線アクセスネットワークについて、説明する。第６の実施の形態の無線アクセスネットワークは、機能構成は第２の実施の形態と同様であるが、図１７に示した状況、つまり、新規無線端末ＭＴ＃ｉが複数の基地局ＡＰ＃１，ＡＰ＃ｋから同時に、あるいは相前後して認証要求応答１を受信した場合に、そのすべてを一旦保持しておき、応答信号の受信レベルが高い基地局から順に認証１の処理を実施し、認証１が成功した基地局を選択し、以降の認証手続きを実行する点に特徴を有する。図２５は、第６の実施の形態において、無線端末ＭＴの基地局選択処理を含むＡＰ認証フローを示している。その他の処理は全て第２の実施の形態と共通である。

【０１４７】無線端末ＭＴの備える機能構成は、図１８に示す第２の実施の形態と同様である。ただし、基地局選択機能３０６が、複数の基地局から認証要求応答１を受信した場合に、そのすべてを一旦保持しておき、応答信号の受信レベルが高い基地局から順に認証１の処理を実施し、認証１が成功した基地局を選択することにより同じ認証処理が同時に複数発生してしまうことを防止する点で第２の実施の形態とは異なる。

【０１４８】次に、第６の実施の形態の無線アクセスネットワークの動作を、図２０の無線端末認証シーケンス、図２５の無線端末の基地局ＡＰ選択処理を含めたＡＰ認証フローを用いて説明する。

【０１４９】ネットワークに一般ユーザが新規に基地局ＡＰ＃ｋを設置した時、ＡＰ＃ｋは事業者が管理する認証サーバＡＳと認証を行うが、この手続きは第１、第２の実施の形態と共通であり、図５の認証シーケンス、図６の認証用パケットペイロードデータ、図７及び図８のＡＰ－ＡＳ間認証フローの通りである。

【０１５０】ある無線端末ＭＴ＃ｉが基地局ＡＰを介してネットワークにアクセスしようとしたとき、ＭＴ＃１は初めにＡＰと認証を行う。基地局ＡＰはこの認証が成功するまで無線端末ＭＴ＃１から送信されたパケットを事業者側ネットワークＮＷに転送しない。なお、第６の実施の形態で用いるＭＴ認証用パケットのペイロードデータは、第１の実施の形態と同様に図１０に示すものである。また、ＡＰ側から見たＭＴ－ＡＰ間認証フローは図１２に、ＭＴ－ＡＳ間認証フローは図１３及び図１４に、中継となる基地局ＡＰ＃ｋ側のＭＴ－ＡＳ間認証フローは図１５及び図１６にそれぞれ示した第１、第２の実施の形態のものと同様である。

【０１５１】図２５に示したＭＴ側から見たＭＴ－ＡＰ間認証フローのステップＳ４０１で、ある無線端末ＭＴ＃ｉがネットワークにアクセスしようとしたとき、鍵生成情報ＫＥｍｔ＃ｉを計算し、その鍵生成情報を添付した認証要求１を基地局ＡＰへブロードキャストで送信する。

【０１５２】第１の実施の形態と同様に、図１２のフローのステップＳ２１１で、無線端末ＭＴ＃１から認証要求１を受信したＡＰ＃ｋは、鍵生成情報ＫＥａｐ＃ｋを計算し、さらにＭＴ＃ｉ－ＡＰ＃ｋ間の共有鍵Ｋｍｔ＃ｉ－ａｐ＃ｋを計算する（ステップＳ２１２）。さらに基地局ＡＰ＃ｋは、乱数Ｒ１を計算し、ＫＥａｐ＃ｋ、Ｒ１を添付した認証要求応答１をＭＴ＃ｉへ送信する（ステップＳ２１３）。

【０１５３】図１７に示した状況では基地局ＡＰ＃１も同じ無線端末ＭＴ＃ｉからの認証要求１を受信するので、同様にして鍵生成情報ＫＥａｐ＃１を計算し、ＭＴ＃ｉ－ＡＰ＃１間の共有鍵Ｋｍｔ＃ｉ－ａｐ＃１を計算する（ステップＳ２１２）。基地局ＡＰ＃１はさらに、乱数Ｒ１’を計算し、ＫＥａｐ＃１、Ｒ１’を添付した認証要求応答１をＭＴ＃ｉへ基地局ＡＰ＃ｋと同様に送信する（ステップＳ２１３）。

【０１５４】図２５のフローのステップＳ４０２，Ｓ４０３で、無線端末ＭＴ＃ｉは予め基地局選択機能３０６に組み込まれたロジック、つまり、送信後の所定時間内に受信した認証要求応答１のうち受信レベルが最も高い基地局を選択するというロジックに基づき基地局を選択し、それ以外の認証処理応答１に対する認証処理は保留にする。ここでは、基地局ＡＰ＃ｋからの認証処理応答１の受信レベルが最高であったとして説明する。

【０１５５】基地局ＡＰ＃１とＡＰ＃ｋとから所定時間内に認証要求応答１を受信した無線端末ＭＴ＃ｉは、受信レベルが高い方の基地局ＡＰ＃ｋからの認証要求応答１に対して処理を行う（ステップＳ４０２～Ｓ４０４’）。他の受信した基地局ＡＰ＃１からの認証処理応答１は、それよりも受信レベルが高い他の基地局について認証１が成功するまでは保持されるが、受信レベルが高い他の基地局が選択された時点で廃棄することにな

る。

【０１５６】図２５のフローのステップＳ４０４′で基地局ＡＰ＃ｋからの認証要求応答１を選択したＭＴ＃ｉは、ステップＳ４０５で、第１、第２の実施の形態と同様に、自装置の鍵生成情報ＫＥｍｔ＃ｉと基地局ＡＰ＃ｋの鍵生成情報ＫＥａｐ＃ｋからＭＴ＃ｉ－ＡＰ＃ｋ間の共有鍵Ｋｍｔ＃ｉ－ａｐ＃ｋを計算する。そして、乱数Ｒ１、自装置の秘密鍵ＳＫｍｔ＃ｉを用いて署名データＳｉｇｍｔ＃ｉを計算する（ステップＳ４０６）。続いて、無線端末ＭＴ＃ｉは乱数Ｒ２を計算し、Ｒ２、自装置の証明書Ｃｅｒｔｍｔ＃ｉ、Ｓｉｇｍｔ＃ｉを認証情報１に添付してそのパケットを選択した基地局ＡＰ＃ｋへ送信する（ステップＳ４０７）。

【０１５７】図１２のフローのステップＳ２１４で、無線端末ＭＴ＃ｉからの認証情報１を受信した基地局ＡＰ＃ｋは、以降、第１、第２の実施の形態と同様の処理を実行し、基地局ＭＴ＃ｉが正規のＭＴであると判断すれば、認証結果１をＭＴ＃ｉへ送信し（ステップＳ２１５～Ｓ２１７）、またＭＴ＃ｉの認証が成功した時点でＭＴ＃ｉから送信される認証２用パケットのＡＳへの転送を許可する（ステップＳ２１８）。一方、もしＭＴの検査に失敗した場合は、認証失敗を示す認証結果１をＭＴ＃ｉへ送信し、ＭＴ＃ｉから送信される認証２用パケットのＡＳへの転送を不許可にする（ステップＳ２１９～Ｓ２２１）。

【０１５８】図２５のフローのステップＳ４０８で基地局ＡＰ＃ｋから認証結果１を受信した無線端末ＭＴ＃ｉは基地局ＡＰ＃ｋの証明書Ｃｅｒｔａｐ＃ｋを検査する（ステップＳ４０９）。この検査が失敗した場合は、当該パケットを破棄し（ステップＳ４１１）、他の基地局からの認証要求応答１を受信しているかどうか判断する（ステップＳ４１２）。

【０１５９】ステップＳ４１２で、他の基地局からの認証要求応答１が残っている場合にはステップＳ４０４′に戻り、残っている認証要求応答１のうち応答信号の受信レベルが最も高い基地局を選択し、ステップＳ４０５以降の処理を繰り返す。図１７の状況では、最初に基地局ＡＰ＃１が選択されることになるが、基地局ＡＰ＃ｋの認証が不成功であれば、次の受信レベルが高い基地局ＡＰ＃１について、ステップＳ４０５以降の処理が実施されることになる。なお、ステップＳ４１２において、他の基地局からの認証要求応答１が残っていない場合には、すべてのパケットを破棄し、ステップＳ４０１に戻り、最初から認証１を開始する。

【０１６０】ステップＳ４０９において、基地局ＡＰ＃ｋの証明書Ｃｅｒｔａｐ＃ｋの検査が成功した場合は、無線端末ＭＴ＃ｉはＣｅｒｔａｐ＃ｋから基地局ＡＰ＃ｋの公開鍵ＰＫａｐ＃ｋを取り出し、このＰＫａｐ＃ｋを用いてＳｉｇａｐ＃ｋを検査し、この検査も成功すれば基地局ＡＰ＃ｋが事業者の認めた正規のＡＰであると判断し、ＭＴ＃ｉ－ＡＰ＃ｋ間の相互認証が完了する。この検査が失敗した場合にも、ステップＳ４１１，Ｓ４１２を実行し、応答信号の受信レベルが２番目に高い基地局ＡＰ＃１からの認証要求応答１に対して同様に認証処理を行う。

【０１６１】上記の認証１が成功したら、無線端末ＭＴ＃ｉは選択した基地局ＡＰ＃ｋを介して認証サーバＡＳと認証を行う。このＭＴ－ＡＳ間の認証手続きは、第１、第２の実施の形態と同様であり、ＭＴ側のＭＴ－ＡＳ間認証フローは図１３に、ＡＰ側のＭＴ－ＡＳ間認証フローは図１４に、中継となる基地局ＡＰ＃ｋ側のＭＴ－ＡＳ間認証フローは図１５及び図１６にそれぞれ示したものである。

【０１６２】この第６の実施の形態の無線アクセスネットワークによれば、第１の実施の形態と同様、基地局ＡＰ＃ｋが無線端末ＭＴ＃ｉの認証が成功するまで事業者側ネットワークにＭＴ＃ｉによるパケットを送信しないので、不正な無線端末による認証を利用した認証サーバＡＳへの攻撃を防止することができ、また、基地局ＡＰを所有するユーザのアクセス回線が不正に利用されることも防止することができる。さらに第６の実施の形態の場合、正規の基地局ＡＰを１つ選択することで同一の認証２用パケットが認証サーバＡＳへ送信されることを防止できる。加えて、応答信号の受信レベルが高い基地局から優先的に選択することで無線通信の信頼性を高めることができ、しかも複数の基地局からの応答を無線端末側で一旦保持しておいて応答信号の受信レベルの高いものから優先して認証処理を実施するので、第２の実施の形態の場合よりも通信処理が迅速化できる。

【０１６３】［第７の実施の形態］次に、本発明の第７の実施の形態の無線アクセスネットワークについて、説明する。第７の実施の形態の無線アクセスネットワークは、機能構成は第２の実施の形態と同様であるが、図１７に示した状況、つまり、新規無線端末ＭＴ＃ｉが複数の基地局ＡＰ＃１，ＡＰ＃ｋから同時に、あるいは相前後して認証要求応答１を受信した場合に、そのすべてを一旦保持しておき、各基地局の帯域使用状況を確認し、帯域の空きが大きい基地局から順に認証１の処理を実施し、認証１が成功した基地局を選択し、以降の認証手続きを実行する点に特徴を有する。図２６は、第７の実施の形態において、無線端末ＭＴの基地局選択処理を含むＡＰ認証フローを示している。その他の処理は全て第２の実施の形態と共通である。

【０１６４】無線端末ＭＴの備える機能構成は、図１８に示す第２の実施の形態と同様である。ただし、基地局選択機能３０６が、複数の基地局から認証要求応答１を受信した場合に、そのすべてを一旦保持しておき、帯域の空きが大きい基地局から順に認証１の処理を実施し、認証１が成功した基地局を選択することにより同じ認証処理が同時に複数発生してしまうことを防止する点で第

２の実施の形態とは異なる。

【０１６５】次に、第７の実施の形態の無線アクセスネットワークの動作を、図２０の無線端末認証シーケンス、図２６の無線端末の基地局ＡＰ選択処理を含めたＡＰ認証フローを用いて説明する。

【０１６６】ネットワークに一般ユーザが新規に基地局ＡＰ＃ｋを設置した時、ＡＰ＃ｋは事業者が管理する認証サーバＡＳと認証を行うが、この手続きは第１、第２の実施の形態と共通であり、図５の認証シーケンス、図６の認証用パケットペイロードデータ、図７及び図８のＡＰ－ＡＳ間認証フローの通りである。

【０１６７】ある無線端末ＭＴ＃ｉが基地局ＡＰを介してネットワークにアクセスしようとしたとき、ＭＴ＃１は初めにＡＰと認証を行う。基地局ＡＰはこの認証が成功するまで無線端末ＭＴ＃１から送信されたパケットを事業者側ネットワークＮＷに転送しない。なお、第７の実施の形態で用いるＭＴ認証用パケットのペイロードデータは、第１の実施の形態と同様に図１０に示すものである。また、ＡＰ側から見たＭＴ－ＡＰ間認証フローは図１２に、ＭＴ－ＡＳ間認証フローは図１３及び図１４に、中継となる基地局ＡＰ＃ｋ側のＭＴ－ＡＳ間認証フローは図１５及び図１６にそれぞれ示した第１、第２の実施の形態のものと同様である。

【０１６８】図２６に示したＭＴ側から見たＭＴ－ＡＰ間認証フローのステップＳ４０１で、ある無線端末ＭＴ＃ｉがネットワークにアクセスしようとしたとき、鍵生成情報ＫＥｍｔ＃ｉを計算し、その鍵生成情報を添付した認証要求１を基地局ＡＰへブロードキャストで送信する。

【０１６９】第１の実施の形態と同様に、図１２のフローのステップＳ２１１で、無線端末ＭＴ＃１から認証要求１を受信したＡＰ＃ｋは、鍵生成情報ＫＥａｐ＃ｋを計算し、さらにＭＴ＃ｉ－ＡＰ＃ｋ間の共有鍵Ｋｍｔ＃ｉ－ａｐ＃ｋを計算する（ステップＳ２１２）。さらに基地局ＡＰ＃ｋは、乱数Ｒ１を計算し、ＫＥａｐ＃ｋ、Ｒ１を添付した認証要求応答１をＭＴ＃ｉへ送信する（ステップＳ２１３）。

【０１７０】図１７に示した状況では基地局ＡＰ＃１も同じ無線端末ＭＴ＃ｉからの認証要求１を受信するので、同様にして鍵生成情報ＫＥａｐ＃１を計算し、ＭＴ＃ｉ－ＡＰ＃１間の共有鍵Ｋｍｔ＃ｉ－ａｐ＃１を計算する（ステップＳ２１２）。基地局ＡＰ＃１はさらに、乱数Ｒ１’を計算し、ＫＥａｐ＃１、Ｒ１’を添付した認証要求応答１をＭＴ＃ｉへ基地局ＡＰ＃ｋと同様に送信する（ステップＳ２１３）。

【０１７１】図２６のフローのステップＳ４０２，Ｓ４０３で、無線端末ＭＴ＃ｉは予め基地局選択機能３０６に組み込まれたロジック、つまり、送信後の所定時間内に受信した認証要求応答１のうち帯域の空きが最も大きい基地局を選択するというロジックに基づき基地局を選択し、それ以外の認証処理応答１に対する認証処理は保留にする。ここでは、基地局ＡＰ＃ｋの帯域の空きが最も大きいとして説明する。

【０１７２】基地局ＡＰ＃１とＡＰ＃ｋとから所定時間内に認証要求応答１を受信した無線端末ＭＴ＃ｉは、帯域の空きが大きい方の基地局ＡＰ＃ｋからの認証要求応答１に対して処理を行う（ステップＳ４０２～Ｓ４０４″）。他の受信した基地局ＡＰ＃１からの認証処理応答１は、帯域の空きがそれよりも大きい他の基地局について認証１が成功するまでは保持されるが、他の基地局が選択された時点で廃棄することになる。

【０１７３】図２６のフローのステップＳ４０４″で基地局ＡＰ＃ｋからの認証要求応答１を選択したＭＴ＃ｉは、ステップＳ４０５で、第１、第２の実施の形態と同様に、自装置の鍵生成情報ＫＥｍｔ＃ｉと基地局ＡＰ＃ｋの鍵生成情報ＫＥａｐ＃ｋからＭＴ＃ｉ－ＡＰ＃ｋ間の共有鍵Ｋｍｔ＃ｉ－ａｐ＃ｋを計算する。そして、乱数Ｒ１、自装置の秘密鍵ＳＫｍｔ＃ｉを用いて署名データＳｉｇｍｔ＃ｉを計算する（ステップＳ４０６）。続いて、無線端末ＭＴ＃ｉは乱数Ｒ２を計算し、Ｒ２、自装置の証明書Ｃｅｒｔｍｔ＃ｉ、Ｓｉｇｍｔ＃ｉを認証情報１に添付してそのパケットを選択した基地局ＡＰ＃ｋへ送信する（ステップＳ４０７）。

【０１７４】図１２のフローのステップＳ２１４で、無線端末ＭＴ＃ｉからの認証情報１を受信した基地局ＡＰ＃ｋは、以降、第１、第２の実施の形態と同様の処理を実行し、基地局ＭＴ＃ｉが正規のＭＴであると判断すれば、認証結果１をＭＴ＃ｉへ送信し（ステップＳ２１５～Ｓ２１７）、またＭＴ＃ｉの認証が成功した時点でＭＴ＃ｉから送信される認証２用パケットのＡＳへの転送を許可する（ステップＳ２１８）。一方、もしＭＴの検査に失敗した場合は、認証失敗を示す認証結果１をＭＴ＃ｉへ送信し、ＭＴ＃ｉから送信される認証２用パケットのＡＳへの転送を不許可にする（ステップＳ２１９～Ｓ２２１）。

【０１７５】図２６のフローのステップＳ４０８で基地局ＡＰ＃ｋから認証結果１を受信した無線端末ＭＴ＃ｉは基地局ＡＰ＃ｋの証明書Ｃｅｒｔａｐ＃ｋを検査する（ステップＳ４０９）。この検査が失敗した場合は、当該パケットを破棄し（ステップＳ４１１）、他の基地局からの認証要求応答１を受信しているかどうか判断する（ステップＳ４１２）。

【０１７６】ステップＳ４１２で、他の基地局からの認証要求応答１が残っている場合にはステップＳ４０４″に戻り、残っている認証要求応答１のうち帯域の空きが最も大きい基地局のものを選択し、ステップＳ４０５以降の処理を繰り返す。図１７の状況では、最初に基地局ＡＰ＃１が選択されることになるが、基地局ＡＰ＃ｋの認証が不成功であれば、次には基地局ＡＰ＃１について、ステップＳ４０５以降の処理が実施されることにな

る。なお、ステップＳ４１２において、他の基地局からの認証要求応答１が残っていない場合には、すべてのパケットを破棄し、ステップＳ４０１に戻り、最初から認証１を開始する。

【０１７７】ステップＳ４０９において、基地局ＡＰ＃ｋの証明書Ｃｅｒｔａｐ＃ｋの検査が成功した場合は、無線端末ＭＴ＃ｉはＣｅｒｔａｐ＃ｋから基地局ＡＰ＃ｋの公開鍵ＰＫａｐ＃ｋを取り出し、このＰＫａｐ＃ｋを用いてＳｉｇａｐ＃ｋを検査し、この検査も成功すれば基地局ＡＰ＃ｋが事業者の認めた正規のＡＰであると判断し、ＭＴ＃ｉ－ＡＰ＃ｋ間の相互認証が完了する。この検査が失敗した場合にも、ステップＳ４１１，Ｓ４１２を実行し、帯域の空きが２番目に大きい基地局ＡＰ＃１からの認証要求応答１に対して同様に認証処理を行う。

【０１７８】上記の認証１が成功したら、無線端末ＭＴ＃ｉは選択した基地局ＡＰ＃ｋを介して認証サーバＡＳと認証を行う。このＭＴ－ＡＳ間の認証手続きは、第１、第２の実施の形態と同様であり、ＭＴ側のＭＴ－ＡＳ間認証フローは図１３に、ＡＰ側のＭＴ－ＡＳ間認証フローは図１４に、中継となる基地局ＡＰ＃ｋ側のＭＴ－ＡＳ間認証フローは図１５及び図１６にそれぞれ示したものである。

【０１７９】この第７の実施の形態の無線アクセスネットワークによれば、第１の実施の形態と同様、基地局ＡＰ＃ｋが無線端末ＭＴ＃ｉの認証が成功するまで事業者側ネットワークにＭＴ＃ｉによるパケットを送信しないので、不正な無線端末による認証を利用した認証サーバＡＳへの攻撃を防止することができ、また、基地局ＡＰを所有するユーザのアクセス回線が不正に利用されることも防止することができる。さらに第７の実施の形態の場合、正規の基地局ＡＰを１つ選択することで同一の認証２用パケットが認証サーバＡＳへ送信されることを防止できる。加えて、使用帯域の空きが大きい基地局から優先的に選択することで無線通信の応答処理速度を高めることができ、しかも複数の基地局からの応答を無線端末側で一旦保持しておいて帯域の空きが大きいものから優先して認証処理を実施するので、第４の実施の形態の場合よりも通信処理が迅速化できる。

【０１８０】［第８の実施の形態］次に、本発明の第８の実施の形態の無線アクセスネットワークについて、図２７～図３２を用いて説明する。第８の実施の形態のシステムは、認証サーバＡＳが径路となる無線端末と基地局の識別子を自装置のデータベースに登録して管理する機能を備えたことを特徴とする。この認証サーバＡＳは、図２７、図２９に示す機能構成であり、図１に示した第１の実施の形態の機能構成に加えて、無線端末移動管理機能１０７を備えている。これに対応する基地局ＭＴは、図２８、図３０に示す機能構成であり、図１に示した第１の実施の形態の機能構成に加えて、リソース開放機能２１０を備えている。

【０１８１】認証サーバＡＳによる無線端末及び基地局の管理機能は次のように実行される。図３１はリソース開放シーケンス、図３２はこのとき使用されるパケットフォーマットを示している。また、ＭＴ登録確認フローは図３３に示している。

【０１８２】第１～第７の実施の形態のいずれかの無線アクセスネットワークで、新規無線端末ＭＴ＃ｉと認証サーバＡＳと間の相互認証が成功した後、図３３のフローに示すように、認証サーバＡＳはその新規無線端末ＭＴ＃ｉと、無線端末－認証サーバ間認証用パケットの中継を行った基地局ＡＰ１，ＡＰ２のそれぞれの識別子ＩＤ（ＭＡＣアドレスを利用するのが好ましいが、本システムで新規に設定するＩＤであってもよい）を対でデータベースに登録し、管理する（ステップＳ５０１）。

【０１８３】また認証サーバＡＳは、この登録時に、新規無線端末ＭＴ＃ｉの識別子ＩＤがすでにデータベースに登録されていないかを確認する（ステップＳ５０２）。もしすでに登録されている場合は、対となる基地局ＡＰ１に対して新規無線端末ＭＴ＃ｉが別の基地局ＡＰ２に移動したことを示すリソース開放通知を送信する（ステップＳ５０３）。

【０１８４】リソース開放通知を受信した基地局ＡＰ１は、リソース開放通知中の無線端末ＭＴの識別子を参照し、対応するリソースを開放し、リソース完了を認証サーバＡＳに送信する。

【０１８５】これにより、第８の実施の形態の無線アクセスネットワークでは、認証サーバＡＳが、自身の認証した無線端末ＭＴ＃ｉの移動を管理し、無線端末がある基地局ＡＰ１から別の基地局ＡＰ２へ移動した時、無線端末－認証サーバ間の相互認証が成功した後に、その無線端末が属していた旧基地局ＡＰ１へ当該無線端末ＭＴ＃ｉが移動したことを通知することにより、基地局が一度は相互認証したがいまでは移動して通信できなくなった無線端末ＭＴ＃ｉの記録をいつまでも保持していなくてもよく、基地局における無線端末の管理データを少なくでき、それだけ処理の高速化が図れる。

【０１８６】［第９の実施の形態］本発明の第９の実施の形態の無線マルチホップネットワークについて、説明する。図３４は本発明の第９の実施の形態の無線マルチホップネットワークの機能構成を示し、図３５は認証サーバＡＳの機能構成、図３６は基地局ＭＴの機能構成、図３７は無線端末ＭＴの機能構成を示している。第９の実施の形態の無線マルチホップネットワークは、パケット中継機能を付加的に備えた無線端末ＭＴ、パケット中継機能を備え、無線端末ＭＴと無線通信する基地局ＡＰ、この基地局ＡＰと事業者側有線ネットワークＮＷを通じて接続される認証サーバＡＳから構成される。

【０１８７】この無線マルチホップネットワークは、図３８に示したように、例えば、無線端末ＭＴ９は、他の

無線端末ＭＴ３，ＭＴ２に中継されて基地局ＡＰ１にアクセスし、この基地局ＡＰ１からネットワークＮＷを通じて認証サーバＡＳに接続され、またその逆の径路でＡＳから無線端末ＭＴ９と通信する。

【０１８８】このため、図３４、図３５に示すように、認証サーバＡＳはソフトウェアとして、無線端末ＭＴとの相互認証を実行する無線端末との認証機能１０１、認証した無線端末ＭＴを、データベースを利用して管理する無線端末管理機能１０２、ネットワークＮＷのパケットを検査する有線区間パケット検査機能１０３、パケット判別を行うパケット判別機能１０４を備え、加えて、基地局との相互認証を実行する基地局との相互認証機能１０５、認証した基地局ＡＰを、データベースを利用して管理する基地局管理機能１０６を備えている。

【０１８９】図３４、図３６に示すように、基地局ＡＰはソフトウェアとして、認証サーバＡＳ－無線端末ＭＴ間の認証用パケットの転送を行う認証用パケット転送機能２０１、無線ネットワークのパケットを検査する無線区間パケット検査機能２０２、有線ネットワークＮＷのパケットを検査する有線区間パケット検査機能２０３、パケット判別を行うパケット判別機能２０４、パケット中継を行うパケット中継機能２０５を備え、加えて、認証サーバＡＳとの相互認証を実行する認証サーバとの相互認証機能２０６、無線端末ＭＴとの相互認証を実行する無線端末との相互認証機能２０７、受信したパケットの転送可否を判断するパケット転送判断機能２０８、認証した無線端末を、データベースによって管理する無線端末管理機能２０９、無線端末選択機能２１１を備えている。

【０１９０】図３４、図３７に示すように、無線端末ＭＴはソフトウェアとして、認証サーバＡＳとの相互認証を実行する認証サーバとの相互認証機能３０１、無線ネットワークのパケットを検査する無線区間パケット検査機能３０２、パケット判別を行うパケット判別機能３０３、他の無線端末からのパケットを中継するパケット中継機能３０４、他の無線端末又は基地局との相互認証を実行する無線端末との相互認証機能３０７、複数の無線端末又は基地局の１つをプロキシ端末として選択する無線端末選択機能３０８、プロキシ端末として選択された場合に認証用パケットを転送する認証用パケット転送機能３０９を備えている。

【０１９１】次に、上記構成の第９の実施の形態の無線マルチホップネットワークの動作について、説明する。図３４及び図３８に示す無線マルチホップネットワークにおいても、基地局ＡＰは事業者また一般ユーザが設置する。そして本ネットワークの場合、無線端末ＭＴは近くの基地局だけでなく近くの無線端末に中継させて事業者ネットワークＮＷに送信することができる。また、このネットワークを実現するため、各無線端末ＭＴは、他の無線端末ＭＴから受信したパケット又は基地局ＡＰから受信したパケットを、宛先のルート上にある隣接するＭＴ又はＡＰへ転送することができる。

【０１９２】＜認証サーバＡＳ－基地局ＡＰ間の相互認証＞ネットワークに一般ユーザが新規に基地局ＡＰ１を設置した時、基地局ＡＰ１は事業者が管理する認証サーバＡＳと認証を行う。この認証シーケンスは第１の実施の形態と同様に図５に示すものであり、認証用パケットペイロードデータは図６に示すものである。また、認証フローも第１の実施の形態と同様で、図７及び図８に示すものとなる。ただし、基地局ＡＰの識別番号が、ここでは＃ｋ＝１であり、ＡＰ＃ｋに代えてＡＰ１を用いる。

【０１９３】初めに図７のフローのステップＳ１０１で、基地局ＡＰ１は鍵生成情報ＫＥａｐ１を計算し、その鍵生成情報を添付した認証要求を送信する。

【０１９４】図８のフローのステップＳ１１１で、基地局ＡＰ１からの認証要求を受信した認証サーバＡＳは、鍵生成情報ＫＥａｓを計算し、ＫＥａｐ１とＫＥａｓからＡＰ１－ＡＳ間の共有鍵Ｋａｐ１－ａｓを計算する（ステップＳ１１２）。認証サーバＡＳはさらに、乱数Ｒ１を計算し、ＫＥａｓ、Ｒ１を添付した認証要求応答を基地局ＡＰ１へ送信する（ステップＳ１１３）。

【０１９５】図７のフローのステップＳ１０２で、認証サーバＡＳからの認証要求応答を受信した基地局ＡＰ１は、自装置の鍵生成情報ＫＥａｐ１と認証サーバＡＳの鍵生成情報ＫＥａｓからＡＰ１－ＡＳ間の共有鍵Ｋａｐ１－ａｓを計算し、乱数Ｒｌと自装置の秘密鍵ＳＫａｐ１を用いて署名データＳｉｇａｐ１を計算する（ステップＳ１０４）。基地局ＡＰ１はさらに乱数Ｒ２を計算し、このＲ２、自装置の証明書Ｃｅｒｔａｐ１、そしてＳｉｇａｐ１を認証情報に添付してそのパケットを認証サーバＡＳへ送信する（ステップＳ１０５）。

【０１９６】図８のフローのステップＳ１１４で、基地局ＡＰ１からの認証情報を受信した認証サーバＡＳは、添付されているＣｅｒｔａｐ１を検査する。もし検査が失敗した場合は、認証失敗を示す認証結果をＡＰ１へ送信する（ステップＳ１１５，Ｓ１１７，Ｓ１１８）。検査が成功した場合は、Ｃｅｒｔａｐ１からＡＰ１の公開鍵ＰＫａｐ１を取り出し、さらにこのＰＫａｐ１を用いてさらに基地局ＡＰ１の種名データＳｉｇａｐ１を検査する。もしこの検査が失敗した場合にも、認証失敗を示す認証結果をＡＰ１へ送信する（ステップＳ１１５，Ｓ１１７，Ｓ１１８）。

【０１９７】そしてこの検査も成功した場合は、基地局ＡＰ１は正規の基地局であると判断し、ステップＳ１１５でＹＥＳに分岐し、乱数Ｒ２、自装置の秘密鍵ＳＫａｓを用いて署名データＳｉｇａｓを計算する（ステップＳ１１６）。認証サーバＡＳはさらに、自装置の証明書Ｃｅｒｔａｓと署名データＳｉｇａｓを認証結果に添付し、そのパケットを基地局ＡＰ１へ送信する（ステップ

Ｓ１１８）。

【０１９８】図7のフローのステップＳ１０６で、認証サーバＡＳからの認証結果を受信した基地局ＡＰ１は、添付されている認証サーバの署名データＣｅｒｔａｓを検査する。もし検査が失敗した場合は、最初から認証処理を開始する（ステップＳ１０７でＮＯに分岐）。この検査が成功した場合は、認証サーバの証明書Ｃｅｒｔａｓから認証サーバＡＳの公開鍵ＰＫａｓを取り出す。基地局ＡＰ１はさらに、取り出した公開鍵ＰＫａｓを用いて認証サーバの署名データＳｉｇａｓを検査する。もし検査が失敗した場合にも、受信した認証結果を破棄し、最初から認証処理を開始する（ステップＳ１０７でＮＯに分岐）。検査が成功した場合は、認証サーバＡＳは事業者が設置した正規の認証サーバであると判断し、ＡＰ１－ＡＳ間の相互認証が完了する（ステップＳ１０７でＹＥＳに分岐）。

【０１９９】このようにして認証サーバＡＳが新規の基地局ＡＰ１を認証することで事業者はユーザが設置したＡＰを把握し、ユーザはそうしたＡＰを事業者が設置したものと同等の安全性を持つとみなして使用することができることになる。

【０２００】＜無線端末ＭＴ－ＭＴ間の相互認証＞図３８に示したネットワークで、無線端末ＭＴ９がネットワークＮＷに初めてアクセスするとき、近隣の無線端末ＭＴ又は基地局ＡＰから認証を受ける。無線端末ＭＴ９の近隣にあるプロキシ端末となる無線端末ＭＴあるいは基地局ＡＰは、ＭＴ９から送信されたパケットを、認証１が成功するまで自装置より先に転送しない。無線端末ＭＴ９の認証シーケンスを図３９に示し、認証用パケットのペイロードデータを図４０に示す。

【０２０１】なお、以下では、無線端末ＭＴ９の近隣には無線端末ＭＴ３，ＭＴ４，ＭＴ８が存在するが、無線端末ＭＴ９は無線端末選択機能３０８によりＭＴ３を選択し、このＭＴ３を最初に中継させ（プロキシ端末とする）、ＭＴ３－ＭＴ２－ＡＰ１のルートで認証サーバＡＳと相互認証手続きを行うようになるものとして説明する。

【０２０２】図４１の無線端末ＭＴ９から見た認証フローにおける最初のステップＳ６０１で、無線端末ＭＴ９は乱数Ｒ１を生成し、Ｒ１を付加した認証要求１をブロードキャストで送信する。図３８の状況ではこの認証要求１は上述したように無線端末ＭＴ３，ＭＴ４，ＭＴ８によって同時に受信される。

【０２０３】図４２のフローのステップＳ６１１で、無線端末ＭＴ９からの認証要求１を受信した無線端末ＭＴ３は、乱数Ｒ２を生成し、自装置の秘密鍵ＳＫｍｔ３と乱数Ｒ１を用いて署名データＳｉｇｍｔ３を計算する（ステップＳ６１２）。無線端末ＭＴ３は続いて、乱数Ｒ２、Ｓｉｇｍｔ３、自装置の証明書Ｃｅｒｔｍｔ３を付加した認証要求応答１を無線端末ＭＴ９に送信する（ステップＳ６１３）。同様に、無線端末ＭＴ９からの認証要求１を受信したＭＴ４、ＭＴ８それぞれも認証要求応答１をＭＴ９に送信する。

【０２０４】図４１のフローのステップＳ６０２で、複数の無線端末ＭＴ３，ＭＴ４，ＭＴ８からの認証要求応答１を受信した無線端末ＭＴ９は、それぞれに添付された証明書（Ｃｅｒｔｍｔ３，Ｃｅｒｔｍｔ４，Ｃｅｒｔｍｔ８）を検査する。検査が失敗した場合は、受信した認証要求応答を破棄する。検査が成功した場合は、その証明書から公開鍵（ＰＫｍｔ３，ＰＫｍｔ４，ＰＫｍｔ８）を取り出し、その公開鍵を用いてそれぞれの署名データ（Ｓｉｇｍｔ３，Ｓｉｇｍｔ４、Ｓｉｇｍｔ８）を検査する（ステップＳ６０３）。

【０２０５】検査が成功した中継ＭＴが１つもない場合には、受信した認証要求応答１を破棄し、最初に戻る（ステップＳ６０４でＮＯに分岐）。

【０２０６】検査が成功した中継ＭＴが１でもある場合には、ステップＳ６０４でＹＥＳに分岐する。そして検査に成功した中継ＭＴが複数ある場合、その中に基地局ＡＰが含まれていれば基地局を優先的にプロキシ（Ｐｒｏｘｙ）端末として選択し、検査に成功したのが無線端末ばかりであれば、新規の無線端末ＭＴ９は基地局ＡＰ１，ＡＰ２までのルート情報ＲＩｎｆｏを調べ、ＡＰまでのホップ数が最も小さい１つのＭＴを選択する。さらに、候補が複数ある場合にはランダムに候補の中から１つの中継ＭＴを選択する（ステップＳ６０５）。ここでは無線端末ＭＴ３が選択されたものとする。なお、候補が複数ある場合に、受信信号レベルが最高の無線端末、あるいは最初に受信した無線端末を選択するようにしてもよい。こうして選択された無線端末ＭＴ３は新規無線端末ＭＴ９のＰｒｏｘｙＭＴとなる。

【０２０７】無線端末ＭＴ９は続いて、乱数Ｒ２と自装置の秘密鍵ＳＫｍｔ９を用いて署名データＳｉｇｍｔ９を計算し、これらＲ２、Ｓｉｇｍｔ９、自装置の証明書Ｃｅｒｔｍｔ９を付加した認証情報１をＰｒｏｘｙＭＴ（ここではＭＴ３）へ送信する（ステップＳ６０６，Ｓ６０７）。

【０２０８】無線端末ＭＴ９により選択された無線端末ＭＴ３は、図４２のフローのステップＳ６１４でＭＴ９からの認証情報１を受信すると、新規無線端末ＭＴ９の証明書Ｃｅｒｔｍｔ９を検査する。もし検査が失敗した場合は、認証失敗を示す認証結果１をＭＴ９へ送信する（ステップＳ６１５，Ｓ６１８～Ｓ６２０）。

【０２０９】検査が成功した場合は、Ｃｅｒｔｍｔ９から公開鍵ＰＫｍｔ９を取り出し、この公開鍵ＰＫｍｔ９を用いて無線端末ＭＴ９の署名データＳｉｇｍｔ９を検査する。もしこの検査が失敗した場合にも、無線端末ＭＴ３は認証失敗を示す認証結果１を無線端末ＭＴ９へ送信し、ＭＴ３はＭＴ９から送信される認証２用パケットのＡＰへの転送を不許可にする（ステップＳ６１５，Ｓ

６１８～Ｓ６２０）。他方、この検査も成功した場合には新規ＭＴ認証成功とし、認証結果１をＭＴ９に送信する（ステップＳ６１５，Ｓ６１６）。この時点で無線端末ＭＴ３は無線端末ＭＴ９から送信される認証２用パケットのＡＰへの転送を許可する（ステップＳ６１７）。

【０２１０】図４１のフローのステップＳ６０８で無線端末ＭＴ９が認証結果１を受信すれば、無線端末ＭＴ９－ＭＴ３間の相互認証が完了する。

【０２１１】このようにして無線マルチホップネットワーク中の認証済みの正規の無線端末ＭＴ３が新規の無線端末ＭＴ９を認証することで、不正無線端末が認証を装って送信したパケットがネットワークへ流入することを防止できる。また新規無線端末は正規のＰｒｏｘｙＭＴを１つ選択することで同一の認証２用パケットが複数発生し、ネットワークＮＷに転送されることを防止できる。

【０２１２】＜無線端末ＭＴ－認証サーバ間の相互認証＞上記の無線端末間の相互認証１の処理が成功したら、無線端末ＭＴ９は無線端末ＭＴ３、基地局ＡＰ１を介して認証サーバＡＳと相互認証を行うことになる。

【０２１３】図４３の新規無線端末ＭＴ側から見た認証フローの初めのステップＳ６２１で、無線端末ＭＴ９はシーケンス番号ＳＱＮを生成し、このＳＱＮと秘密鍵ＳＫｍｔ９を用いてパケット検査データＰＣＶを計算し、これらのＳＱＮ、ＰＣＶを付加した認証要求２を無線端末ＭＴ３へ送信する（ステップＳ６２２）。

【０２１４】図４５のＰｒｏｘｙＭＴ側から見た認証フローのステップＳ６６１で、無線端末ＭＴ９からの認証要求２を受信した無線端末ＭＴ３は、それに添付されているＰＣＶをシーケンス番号ＳＱＮ、公開鍵ＰＫｍｔ９を用いて検査する（ステップＳ６５１）。もし検査が失敗した場合は、受信した認証要求２を破棄する。検査が成功した場合は、無線端末ＭＴ３はＳＱＮと認証済み装置に配布されている無線マルチホップネットワークで共通のネットワーク鍵ＮＫ（共有鍵）を用いてパケット検査データＰＣＶを計算する（ステップＳ６５２）。続いて無線端末ＭＴ３は、元のＰＣＶを廃棄し、新しく計算したＰＣＶを付加した認証要求２をルート上の次装置（ここでは無線端末ＭＴ２）へ送信する（ステップＳ６５３）。

【０２１５】図４６のフローのステップＳ６７１で、中継となる無線端末ＭＴ３は、無線端末ＭＴ９からの認証要求２を受信すれば、シーケンス番号ＳＱＮとネットワーク鍵ＮＫを用いてパケット検査データＰＣＶを検査し、失敗した場合は受信した認証要求２を破棄し、成功した場合はルート上の次の装置である無線端末ＭＴ２へパケットをそのまま送信する（ステップＳ６７２）。同様に、次の装置である無線端末ＭＴ２も、中継となる無線端末ＭＴ３から認証要求２を受信すれば、ＳＱＮとＮＫを用いてＰＣＶを検査し、失敗した場合は受信した認証要求２を破棄し、成功した場合はルート上の次の装置である基地局ＡＰ１へパケットをそのまま送信する（ステップＳ６７２）図４５のフローのステップＳ６５１で、無線端末ＭＴ２から認証要求２を受信した基地局ＡＰ１は、パケット検査データＰＣＶをシーケンス番号ＳＱＮ、ネットワーク鍵ＮＫを用いて検査する。もし検査が失敗した場合は、受信した認証要求２を破棄する。検査が成功した場合は、ＳＱＮと共有鍵Ｋａｐ１－ａｓを用いてＰＣＶを計算し（ステップＳ６５２）、元のＰＣＶを廃棄して新しいＰＣＶを付加した認証要求２を認証サーバＡＳへ送信する（ステップＳ６５３）。

【０２１６】図４４に示されている認証サーバＡＳ側から見た認証フローのステップＳ６３１で、基地局ＡＰ１から認証要求２を受信した認証サーバＡＳは、ＰＣＶをＳＱＮ、Ｋａｐ１－ａｓを用いて検査する（ステップＳ６３２）。もし検査が失敗した場合、認証サーバＡＳは受信した認証要求２を破棄する。検査が成功した場合、認証サーバＡＳは続いて乱数Ｒ３を計算し、シーケンス番号ＳＱＮを生成し、そのＳＱＮ、共有鍵Ｋａｐ１－ａｓを用いてパケット検査データＰＣＶを計算し、乱数Ｒ３とＳＱＮ、ＰＣＶを付加した認証要求応答２を基地局ＡＰ１へ送信する（ステップＳ６３３，Ｓ６３４）。

【０２１７】図４５のフローのステップＳ６５１で、認証サーバＡＳからの認証要求応答２を受信した基地局ＡＰ１は、シーケンス番号ＳＱＮ、共有鍵Ｋａｐ１－ａｓを用いてパケット検査データＰＣＶを検査する。もし検査が失敗した場合は受信した認証要求応答２を破棄する。検査が成功した場合は、基地局ＡＰ１は、シーケンス番号ＳＱＮとネットワーク鍵ＮＫを用いて新たにパケット検査データＰＣＶを計算し、元のＰＣＶを破棄し、新たに計算したＰＣＶを付加した認証要求応答２を中継となる無線端末ＭＴ２へ送信する（ステップＳ６５２，Ｓ６５３）。

【０２１８】図４６のフローのステップＳ６７１で、基地局ＡＰ１からの認証要求応答２を受信した中継無線端末ＭＴ２は、ＳＱＮとＮＫを用いてＰＣＶを検査し、検査が失敗した場合は受信した認証要求応答２を破棄し、検査が成功した場合はそのまま次の中継となる無線端末ＭＴ３へ送信する（ステップＳ６７２）。

【０２１９】ＰｒｏｘｙＭＴとなっている無線端末ＭＴ３は、図４５のフローのステップＳ６５１で無線端末ＭＴ２からの認証要求応答２を受信すれば、シーケンス番号ＳＱＮ、ネットワーク鍵ＮＫを用いてパケット検査データＰＣＶを検査し、この検査が成功した場合には、ＳＱＮと秘密鍵ＳＫｍｔ３を用いて新たにＰＣＶを計算し、元のＰＣＶを破棄し、新しいＰＣＶを付加した認証要求応答２を新規無線端末ＭＴ９へ送信する（ステップＳ６５２，Ｓ６５３）。

【０２２０】図４３のフローのステップＳ６２３で、無線端末ＭＴ３からの認証要求応答２を受信した新規無線

端末ＭＴ９は、パケット検査データＰＣＶをシーケンス番号ＳＱＮ、公開鍵ＰＫｍｔ３を用いて検査する（ステップＳ６２４）。もし検査が失敗した場合、無線端末ＭＴ９は受信した認証要求応答２を破棄し、最初から認証２を開始する。検査が成功した場合、無線端末ＭＴ９は乱数Ｒ３、秘密鍵ＳＫｍｔ９を用いて署名データＳｉｇｍｔ９を計算する（ステップＳ６２５）。無線端末ＭＴ９は続いて乱数Ｒ４を計算し、この乱数Ｒ４、自装置の証明書Ｃｅｒｔｍｔ９、署名データＳｉｇｍｔ９及び上記と同様の手順で計算したパケット検査データＰＣＶを認証情報２に付加してそのパケットを無線端末ＭＴ３へ送信する（ステップＳ６２６，Ｓ６２７）。

【０２２１】図４５のフローのステップＳ６５１で、認証情報２を受信したＰｒｏｘｙ無線端末ＭＴ３は、ＰＣＶを検査し、結果が正しければ新しいＰＣＶを付加して認証情報２を次の中継とする無線端末ＭＴ２へ送信する（ステップＳ６５２，Ｓ６５３）。

【０２２２】次の中継となる無線端末ＭＴ２は、図４６のフローのステップＳ６７１で無線端末ＭＴ３からの認証情報２を受信すれば、ＰＣＶを検査し、検査結果が正しければそのまま認証結果２を基地局ＡＰ１へ送信する（ステップＳ６７２）。

【０２２３】図４５のフローのステップＳ６５１で、無線端末ＭＴ２からの認証情報２を受信した基地局ＡＰ１は、ＰＣＶを検査し、結果が正しければ新しいＰＣＶを付加して認証結果２のパケットを認証サーバＡＳへ送信する（ステップＳ６５２，Ｓ６５３）。

【０２２４】図４４のフローのステップＳ６３５で基地局ＡＰ１からの認証情報２を受信した認証サーバＡＳは、ＰＣＶを検査する（ステップＳ６３６）。もし検査が失敗した場合、ＡＳは受信した認証情報２を破棄する。検査が成功した場合、ＡＳは無線端末ＭＴ９の証明書Ｃｅｒｔｍｔ９を検査する（ステップＳ６３７）。もし検査が失敗した場合、ＡＳは認証失敗を示す認証結果２を新しいＰＣＶを付加して基地局ＡＰ１へ送信する（ステップＳ６３７，Ｓ６４１～Ｓ６４３）。

【０２２５】無線端末ＭＴ９の証明書Ｃｅｒｔｍｔ９の検査が成功した場合、認証サーバＡＳはＣｅｒｔｍｔ９から無線端末ＭＴ９の公開鍵ＰＫｍｔ９を取り出し、さらにこのＰＫｍｔ９を用いてＳｉｇｍｔ９を検査する。もし検査が失敗した場合は、認証失敗を示す認証結果２を新しいＰＣＶを付加して基地局ＡＰ１へ送信する（ステップＳ６３７，Ｓ６４１～Ｓ６４３）。検査が成功すれば無線端末ＭＴ９は正規のＭＴであると判断し、認証サーバＡＳは乱数Ｒ４、自装置の秘密鍵ＳＫａｓを用いて署名データＳｉｇａｓを計算する（ステップＳ６３７，Ｓ６３８）。

【０２２６】次に認証サーバＡＳは、ネットワーク鍵ＮＫを無線端末ＭＴ９の公開鍵ＰＫｍｔ９で暗号化し、自装置の証明書Ｃｅｒｔａｓと署名データＳｉｇａｓ、新しいＰＣＶ、暗号化したネットワーク鍵ＮＫを認証結果２に付加し（ステップＳ６３９）、そのパケットを基地局ＡＰ１へ送信する（ステップＳ６４０）。

【０２２７】認証サーバＡＳからの認証結果２を受信すれば、基地局ＡＰ１は図４５のフローのステップＳ６５１でＰＣＶを検査する。この検査結果が正しければ新しいＰＣＶを付加して認証結果２をＭＴ２へ送信する（ステップＳ６５２，Ｓ６５３）。

【０２２８】図４６のフローのステップＳ６７１で、中継となる無線端末ＭＴ２は基地局ＡＰ１からの認証結果２を受信すればＰＣＶを検査し、結果が正しければそのまま認証結果２を次の無線端末ＭＴ３へ送信する（ステップＳ６７２）。

【０２２９】図４５のフローのステップＳ６５１で、無線端末ＭＴ３は無線端末ＭＴ２からの認証結果２を受信すればＰＣＶを検査し、結果が正しければ新しいＰＣＶを認証結果２に付加し、そのパケットを新規の無線端末ＭＴ９へ送信する（ステップＳ６５２，Ｓ６５３）。

【０２３０】図３３のフローのステップＳ６２８で、Ｐｒｏｘｙ無線端末ＭＴ３からの認証結果２を受信した無線端末ＭＴ９は、ＰＣＶを検査する（ステップＳ６２９）。もし検査が失敗した場合、無線端末ＭＴ９は認証情報２を再送する。ＰＣＶの検査が成功した場合、無線端末ＭＴ９はさらに認証サーバＡＳの証明書Ｃｅｒｔａｓを検査する。もし検査が失敗した場合、無線端末ＭＴ９は最初から認証２を開始する（ステップＳ６３０でＮＯに分岐）。検査が成功した場合、無線端末ＭＴ９は認証サーバの証明書Ｃｅｒｔａｓから認証サーバＡＳの公開鍵ＰＫａｓを取り出し、このＰＫａｓを用いて認証サーバの署名データＳｉｇａｓを検査する。もしこの検査が失敗した場合にも、無線端末ＭＴ９は最初から認証２を開始する（ステップＳ６３０でＮＯに分岐）。この検査が成功すれば、無線端末ＭＴ９は最終的に認証サーバＡＳは事業者が設置した正規のＡＳであると判断し、ネットワーク鍵ＮＫを秘密鍵ＳＫｍｔ９を用いて復号化して保存し、無線端末ＭＴ９－認証サーバＡＳ間の相互認証が完了する（ステップＳ６３０でＹＥＳに分岐）。

【０２３１】本発明の第９の実施の形態の無線マルチホップネットワークでは、上記のように認証２用パケットにパケット検査データ（ＰＣＶ）を付加することで経路上の無線端末ＭＴ、基地局ＡＰは正規のＭＴから送信されたパケットであることを確認するようにしたので、認証２を利用した攻撃を防止することができる。また、認証サーバＡＳは無線端末ＭＴから送信された認証２用パケットが正規の基地局ＡＰを経由して送信されたことを確認できる。さらに、基地局ＡＰが無線端末ＭＴを認証した後に認証サーバＡＳがＭＴを認証することで、事業者はどの基地局ＡＰにどの無線端末ＭＴがアクセスしているかを把握できる。

【０２３２】［第１０の実施の形態］第９の実施の形態

では、図４１にフローに示したＭＴ間の認証処理の新規ＭＴ側の処理において、ステップＳ６０２の認証要求応答１の受信により、複数の無線端末及び基地局からの応答を受信した場合、ステップＳ６０３でそのすべてについて認証処理を実行し、認証が成功した無線端末が複数ある場合には、ステップＳ６０５において基地局を優先的に選択し、また基地局が含まれていない場合には複数の無線端末のうち、基地局までのホップ数が最小のものを選択するようにした。しかしながら、複数の無線端末、基地局からＰｒｏｘｙ端末を選択するロジックはこれに限らず、例えば、基地局、無線端末を区別せず、最先に応答を受信した基地局又は無線端末から順に認証処理を行い、認証が成功した無線端末又は基地局をＰｒｏｘｙ端末として選択する方法を採用することもできる。

【０２３３】第１０の実施の形態の無線マルチホップネットワークは、この選択手順を採用したことを特徴とする。すなわち、第９の実施の形態と同様に図３４～図３７の機能構成を有する無線マルチホップネットワークにおいては、各無線端末ＭＴの無線端末選択機能３０８が図４７のＭＴ間認証処理を実施する。

【０２３４】図３８に示す状況において、新規の無線端末ＭＴ９がブロードキャストで認証要求１を送信し（ステップＳ６０１）、複数の無線端末や基地局から認証要求応答１が返信されてきたとする。ここでは、複数の無線端末ＭＴ３，ＭＴ４，ＭＴ８からの認証要求応答１を受信したとする（ステップＳ６０２）。

【０２３５】このとき無線端末ＭＴ９は、まず、最先に応答を受信した無線端末又は基地局を選択する（ここでは無線端末ＭＴ３を選択したとする。ステップＳ６０４－１）。そして、その認証要求応答１に添付された証明書Ｃｅｒｔｍｔ３を検査する（ステップＳ６０４－２）。検査が失敗した場合は、受信した認証要求応答１を破棄し、次に応答を受信した無線端末又は基地局を選択して再度証明書の検査を実施する手順を繰り返す（ステップＳ６０４－１，Ｓ６０４－２，Ｓ６０４－３）。

【０２３６】ステップＳ６０４－２で証明書の検査が成功した場合は、その証明書から公開鍵ＰＫｍｔ３を取り出し、その公開鍵を用いて署名データＳｉｇｍｔ３を検査する（ステップＳ６０４－２）。この検査が失敗した場合にも、受信した認証要求応答１を破棄し、次に応答を受信した無線端末又は基地局を選択して再度証明書の検査を実施する手順を繰り返す（ステップＳ６０４－１，Ｓ６０４－２，Ｓ６０４－３）。そして、両方の検査が成功した中継ＭＴが１つもない場合には、最初に戻り、認証要求１のブロードキャストからやり直す（ステップＳ６０４－３でＮＯに分岐）。両方の検査が成功した中継ＭＴがあれば、ステップＳ６０４－２でＹＥＳに分岐する。ここでも、無線端末ＭＴ３が選択されたものとする（ステップＳ６０５）。

【０２３７】無線端末ＭＴ９は続いて、乱数Ｒ２と自装置の秘密鍵ＳＫｍｔ９を用いて署名データＳｉｇｍｔ９を計算し、これらＲ２、Ｓｉｇｍｔ９、自装置の証明書Ｃｅｒｔｍｔ９を付加した認証情報１をＰｒｏｘｙＭＴ（ここではＭＴ３）へ送信する（ステップＳ６０６，Ｓ６０７）。

【０２３８】無線端末ＭＴ９により選択された無線端末ＭＴ３は、以降、第９の実施の形態と同様に図４２のフローのステップＳ６１４でＭＴ９からの認証情報１を受信すると、新規無線端末ＭＴ９の証明書Ｃｅｒｔｍｔ９を検査する。もし検査が失敗した場合は、認証失敗を示す認証結果１をＭＴ９へ送信する（ステップＳ６１５，Ｓ６１８～Ｓ６２０）。

【０２３９】検査が成功した場合は、Ｃｅｒｔｍｔ９から公開鍵ＰＫｍｔ９を取り出し、この公開鍵ＰＫｍｔ９を用いて無線端末ＭＴ９の署名データＳｉｇｍｔ９を検査する。もしこの検査が失敗した場合にも、無線端末ＭＴ３は認証失敗を示す認証結果１を無線端末ＭＴ９へ送信し、ＭＴ３はＭＴ９から送信される認証２用パケットのＡＰへの転送を不許可にする（ステップＳ６１５，Ｓ６１８～Ｓ６２０）。他方、この検査も成功した場合には新規ＭＴ認証成功とし、認証結果１をＭＴ９に送信する（ステップＳ６１５，Ｓ６１６）。この時点で無線端末ＭＴ３は無線端末ＭＴ９から送信される認証２用パケットのＡＰへの転送を許可する（ステップＳ６１７）。

【０２４０】図４１のフローのステップＳ６０８で無線端末ＭＴ９が認証結果１を受信すれば、無線端末ＭＴ９－ＭＴ３間の相互認証が完了する。

【０２４１】このようにして無線マルチホップネットワーク中の認証済みの正規の無線端末ＭＴ３が新規の無線端末ＭＴ９を認証することで、不正無線端末が認証を装って送信したパケットがネットワークへ流入することを防止できる。また新規無線端末は正規のＰｒｏｘｙＭＴあるいは基地局を１つ選択することで同一の認証２用パケットが複数発生し、ネットワークＮＷに転送されることを防止できる。加えて、第１０の実施の形態の場合、最先に応答のあった無線端末又は基地局から優先的にプロキシ端末として選択することで、実質的な通信処理速度を速めることができる。

【０２４２】［第１１の実施の形態］本発明の第１１の実施の形態の無線マルチホップネットワークについて、図４８を用いて説明する。第１１の実施の形態の無線マルチホップネットワークは、第９の実施の形態と同様に図３４～図３７の機能構成を有する無線マルチホップネットワークにおいては、各無線端末ＭＴの無線端末選択機能３０８が図４８のＭＴ間認証処理を実施することを特徴とする。

【０２４３】すなわち、新規の無線端末ＭＴがＭＴ間の認証処理において、複数の無線端末、基地局から認証要求応答１を受信した場合に、受信レベルの高い基地局又は無線端末から順に認証処理を行い、認証が成功した無

線端末又は基地局をＰｒｏｘｙ端末として選択するようにしたことを特徴とする。

【０２４４】図３８に示す状況において、新規の無線端末ＭＴ９がブロードキャストで認証要求１を送信し（ステップＳ６０１）、複数の無線端末や基地局から認証要求応答１が返信されてきたとする。ここでは、複数の無線端末ＭＴ３，ＭＴ４，ＭＴ８からの認証要求応答１を受信したとする（ステップＳ６０２）。

【０２４５】このとき無線端末ＭＴ９は、まず、応答信号の受信レベルの最も高い無線端末又は基地局を選択する（ここでも無線端末ＭＴ３を選択したとする。ステップＳ６０４－１１）。そして、その認証要求応答１に添付された証明書Ｃｅｒｔｍｔ３を検査する（ステップＳ６０４－２）。検査が失敗した場合は、受信した認証要求応答１を破棄し、次に応答を受信した無線端末又は基地局を選択して再度証明書の検査を実施する手順を繰り返す（ステップＳ６０４－１１，Ｓ６０４－２，Ｓ６０４－３）。

【０２４６】ステップＳ６０４－２で証明書の検査が成功した場合は、その証明書から公開鍵ＰＫｍｔ３を取り出し、その公開鍵を用いて署名データＳｉｇｍｔ３を検査する。この検査が失敗した場合にも、受信した認証要求応答１を破棄し、次に応答を受信した無線端末又は基地局を選択して再度証明書の検査を実施する手順を繰り返す（ステップＳ６０４－１１，Ｓ６０４－２，Ｓ６０４－３）。そして、両方の検査が成功した中継ＭＴが１つもない場合には、最初に戻り、認証要求１のブロードキャストからやり直す（ステップＳ６０４－３でＮＯに分岐）。

【０２４７】両方の検査が成功した中継ＭＴがあれば、ステップＳ６０４－２でＹＥＳに分岐する。ここでも、無線端末ＭＴ３が選択されたものとする（ステップＳ６０５）。以降の処理は第１０の実施の形態と共通である。

【０２４８】このようにして無線マルチホップネットワーク中の認証済みの正規の無線端末ＭＴ３が新規の無線端末ＭＴ９を認証することで、不正無線端末が認証を装って送信したパケットがネットワークへ流入することを防止できる。また新規無線端末は正規のＰｒｏｘｙＭＴあるいは基地局を１つ選択することで同一の認証２用パケットが複数発生し、ネットワークＮＷに転送されることを防止できる。加えて、第１１の実施の形態の場合、応答信号の受信レベルが高い無線端末又は基地局から優先的にプロキシ端末として選択することで、通信の信頼性を高めることができる。

【０２４９】［第１２の実施の形態］本発明の第１２の実施の形態の無線マルチホップネットワークについて、図４９を用いて説明する。第１２の実施の形態の無線マルチホップネットワークは、第９の実施の形態と同様に図３４～図３７の機能構成を有する無線マルチホップネットワークにおいては、各無線端末ＭＴの無線端末選択機能３０８が図４９のＭＴ間認証処理を実施することを特徴とする。

【０２５０】すなわち、新規の無線端末ＭＴがＭＴ間の認証処理において、複数の無線端末、基地局から認証要求応答１を受信した場合に、基地局ＡＰまでのホップ数が最も少ない無線端末から順に認証処理を行い、認証が成功した無線端末又は基地局をＰｒｏｘｙ端末として選択するようにしたことを特徴とする。

【０２５１】図３８に示す状況において、新規の無線端末ＭＴ９がブロードキャストで認証要求１を送信し（図４９のステップＳ６０１）、複数の無線端末や基地局から認証要求応答１が返信されてきたとする。ここでは、複数の無線端末ＭＴ３，ＭＴ４，ＭＴ８からの認証要求応答１を受信したとする（ステップＳ６０２）。

【０２５２】このとき無線端末ＭＴ９は、基地局までのホップ数が最も少ない無線端末を選択し、又は基地局からの認証要求応答１を直接に受信したのであればその基地局をそのまま選択する（ここでも無線端末ＭＴ３を選択したとする。ステップＳ６０４－２１）。そして、その認証要求応答１に添付された証明書Ｃｅｒｔｍｔ３を検査する（ステップＳ６０４－２）。検査が失敗した場合は、受信した認証要求応答１を破棄し、基地局までのホップ数がその次に少ない無線端末を選択して再度証明書の検査を実施する手順を繰り返す（ステップＳ６０４－１１，Ｓ６０４－２，Ｓ６０４－３）。

【０２５３】ステップＳ６０４－２で証明書の検査が成功した場合は、その証明書から公開鍵ＰＫｍｔ３を取り出し、その公開鍵を用いて署名データＳｉｇｍｔ３を検査する。この検査が失敗した場合にも、受信した認証要求応答１を破棄し、基地局までのホップ数がその次に少ない無線端末を選択して再度証明書の検査を実施する手順を繰り返す（ステップＳ６０４－２１，Ｓ６０４－２，Ｓ６０４－３）。そして、両方の検査が成功した中継ＭＴが１つもない場合には、最初に戻り、認証要求１のブロードキャストからやり直す（ステップＳ６０４－３でＮＯに分岐）。

【０２５４】両方の検査が成功した中継ＭＴがあれば、ステップＳ６０４－２でＹＥＳに分岐する。ここでも、無線端末ＭＴ３が選択されたものとする（ステップＳ６０５）。以降の処理は第１０の実施の形態と共通である。

【０２５５】このようにして無線マルチホップネットワーク中の認証済みの正規の無線端末ＭＴ３が新規の無線端末ＭＴ９を認証することで、不正無線端末が認証を装って送信したパケットがネットワークへ流入することを防止できる。また新規無線端末は正規のＰｒｏｘｙＭＴあるいは基地局を１つ選択することで同一の認証２用パケットが複数発生し、ネットワークＮＷに転送されることを防止できる。加えて、第１２の実施の形態の場合、

基地局までのホップ数が少ない無線端末から優先的にプロキシ端末として選択することで、通信の信頼性と応答速度を高めることができる。

【０２５６】なお、本発明は上記のすべての実施の形態において無線端末、基地局、認証サーバそれぞれが果たす図示フローチャート各々の諸機能を実現させるために各装置に組み込んで実行させるソフトウェアプログラムも権利対象とするものである。

【０２５７】

【発明の効果】請求項１の発明の無線アクセスネットワークによれば、認証サーバ（ＡＳ）と基地局（ＡＰ）が相互認証を行うことで、事業者が一般ユーザの設置したＡＰの安全性を保障することができる。また、新規無線端末（ＭＴ）がアクセスしたとき、最初にＭＴ－ＡＰ間で相互認証することで互いが正当な装置であるか否かを確認することができ、ＡＰはこの相互認証が成功するまでは新規ＭＴが送信したパケットを事業者側ネットワークに転送しないので、認証を装ったＤｏＳ攻撃を防止することができる。さらに、ＭＴ－ＡＰ間の相互認証成功後にＭＴ－ＡＳ間の相互認証及びこの認証用パケットのパケット検査（送信元確認）を行うことで、ＡＳはどのＡＰにどのＭＴがアクセスしたかを正確に把握して管理することができる。

【０２５８】請求項２の発明の無線マルチホップネットワークによれば、新規無線端末（ＭＴ）が無線マルチホップネットワークにアクセスしたとき、最初に新規ＭＴ－近隣ＭＴ間で相互認証することで互いが正当な装置であるか否かを確認することができ、近隣のＭＴはこの相互認証が成功するまでは新規ＭＴが送信したパケットを無線マルチホップネットワークに転送しないので、認証を装ったＤｏＳ攻撃を防止することができる。また、相互認証の際にＭＴ－ＡＳ（認証サーバ）間相互認証用パケットを中継させるＭＴ又はＡＰ（基地局）を１つ選択することで、同じ認証処理が同時に複数発生してしまうことを防止する。さらに、ＭＴ－ＡＰ間の相互認証成功後にＭＴ－ＡＳ間の相互認証及びこの認証用パケットのパケット検査（送信元確認）を行うことでＡＳはどのＡＰにどのＭＴがアクセスしたかを正確に把握して管理することができる。

【０２５９】請求項３の発明の無線端末（ＭＴ）によれば、無線アクセスネットワークに新規に参入するときに基地局（ＡＰ）と相互認証を行い、その成功の後に認証サーバ（ＡＳ）と相互認証を行う機能を備えたことで、ＡＰに新規ＭＴとの相互認証が成功するまで新規ＭＴの送信したパケットを事業者側ネットワークに転送しない機能を持たせることによって、当該ＭＴを用いなければＡＰとの通信、ひいては認証サーバ（ＡＳ）との通信ができない無線アクセスネットワークを構築することができ、認証を装ったＤｏＳ攻撃に耐性の強い無線アクセスネットワークの構築に寄与できる。

【０２６０】請求項４の発明の無線端末によれば、送信する認証用パケットに送信元を示すパケット検査データを算出して添付する機能を備えたので、認証用パケットにパケット検査データを添付することにより、受信先の基地局に送信元を明かすことができ、不正な攻撃のために用いられなくできる。

【０２６１】請求項５～８の発明の無線端末（ＭＴ）によれば、新規ＭＴはＭＴ－ＡＰ（基地局）間相互認証の際にＭＴ－ＡＳ（認証サーバ）間相互認証用パケットを中継させるＡＰ又はＭＴを所定のロジックにしたがって選択することで、同じ認証処理が同時に複数発生してしまうことを防止することができる。

【０２６２】請求項９の発明の認証サーバ（ＡＳ）によれば、基地局（ＡＰ）と相互認証を行い、また新規無線端末（ＭＴ）とも相互認証を行い、しかも新規無線端末との相互認証の際には認証用パケットに添付されている送信元を示すパケット検査データを検査し、この検査が成功すれば相互認証を実施することになるので、不正なＡＰを排除し、正規のＡＰだけを管理することができ、またどのＡＰにどのＭＴがアクセスしたかをも正確に把握することができる。

【０２６３】請求項１０の発明の認証サーバ（ＡＳ）によれば、自身の認証した無線端末（ＭＴ）の移動を管理し、ＭＴがある基地局（ＡＰ）から別のＡＰへ移動した時、ＭＴ－ＡＳ間の相互認証が成功した後に、そのＭＴが属していた旧ＡＰへ当該ＭＴが移動したことを通知することにより、ＡＰに一度は相互認証したがいまでは移動して通信できなくなったＭＴの記録をいつまでも保持させなくてもよく、ＡＰにおけるＭＴの管理データを少なくでき、それだけ処理の高速化が図れる。

【０２６４】請求項１１の発明の基地局（ＡＰ）によれば、新規に無線アクセスネットワーク又は無線マルチホップネットワークに接続するときには必ず認証サーバと相互認証を実施するため、不正にＡＰを設置することを困難にし、事業者が一般ユーザの設置したＡＰの安全性を保障することができる。

【０２６５】請求項１２の発明の基地局（ＡＰ）によれば、新規無線端末（ＭＴ）がアクセスしてきたとき、最初にＭＴ－ＡＰ間で相互認証することでＭＴが正当な装置であるか否かを確認し、この相互認証が成功するまでは新規ＭＴが送信したパケットを事業者側ネットワークに転送しないので、認証を装ったＤｏＳ攻撃を防止することができる。

【０２６６】請求項１３の発明の基地局によれば、相互認証に成功した無線端末それぞれの情報を自装置に登録する機能と、認証サーバから移動通知を受けて、該当する無線端末の登録情報を削除する機能とを備えたので、無線端末が他の基地局の通信エリアに移動した場合に、通信ができなくなってしまった無線端末の情報を削除することによって無線端末の管理のためのリソースを節約

できる。

【０２６７】請求項１４の発明の無線端末（ＭＴ）によれば、無線マルチホップネットワークに新規にアクセスするとき、最初に近隣ＭＴ又はＡＰとの間で相互認証する機能を備えたことで、当該ＭＴが新規に無線マルチホップネットワークに参入する際には近隣のＭＴ又はＡＰに正当な装置であるか否かを確認させ、近隣のＭＴ又はＡＰはこの相互認証が成功するまでは当該ＭＴが送信したパケットを無線マルチホップネットワークに転送しないので、認証を装ったＤｏＳ攻撃に対する耐性の高い無線マルチホップネットワークの構築に寄与できる。また、相互認証の際にＭＴ－ＡＳ（認証サーバ）間相互認証用パケットを中継させるＭＴ又はＡＰ（基地局）を１つ選択する機能を備えたことで、同じ認証処理が同時に複数発生してしまうことを防止することができる。

【０２６８】請求項１５の発明の無線端末（ＭＴ）によれば、自装置が新規に無線マルチホップネットワークにアクセスするときに、無線端末間認証用パケットを近隣の無線端末又は基地局に送信する機能と、自装置が新規無線端末である場合に、無線端末－認証サーバ間認証用パケットに送信元を示すパケット検査データを添付して送信する機能と、自装置が他の新規無線端末によって選択されたプロキシ端末である場合には、他の新規無線端末から送信された無線端末－認証サーバ間認証用パケットに対してパケット検査データを検査し、検査が失敗すればその認証用パケットを破棄し、当該検査が成功すれば当該認証用パケットに自装置で算出した送信元を示すパケット検査データを添付してルート上の他の無線端末又は基地局に対して転送する機能とを備えたので、どの基地局（ＡＰ）にどの無線端末（ＭＴ）がアクセスしたかを認証サーバに正確に把握させることができる。

【０２６９】請求項１６～１８の発明の無線端末（ＭＴ）によれば、ＭＴ－ＡＰ（基地局）間相互認証の際にＭＴ－ＡＳ（認証サーバ）間相互認証用パケットを中継させるＡＰ又はＭＴとして最適なものを選択する機能を備えたことで、同じ認証処理が同時に複数発生してしまうことを防止することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態の無線アクセスネットワークの機能構成のブロック図。

【図２】第１の実施の形態における認証サーバの機能ブロック図。

【図３】第１の実施の形態における基地局の機能ブロック図。

【図４】第１の実施の形態における無線端末の機能ブロック図。

【図５】第１の実施の形態における基地局（ＡＰ）－認証サーバ（ＡＳ）間の認証シーケンス図。

【図６】第１の実施の形態におけるＡＰ－ＡＳ間の認証用パケットのペイロードデータの説明図。

【図７】第１の実施の形態において実施するＡＰ－ＡＳ間認証におけるＡＰ側の認証処理のフローチャート。

【図８】第１の実施の形態において実施するＡＰ－ＡＳ間認証におけるＡＳ側の認証処理のフローチャート。

【図９】第１の実施の形態における無線端末（ＭＴ）－認証サーバ（ＡＳ）間の認証シーケンス図。

【図１０】第１の実施の形態におけるＭＴ－ＡＳ間の認証用パケットのペイロードデータの説明図。

【図１１】第１の実施の形態において実施するＭＴ－ＡＰ間認証におけるＭＴ側の認証処理のフローチャート。

【図１２】第１の実施の形態において実施するＭＴ－ＡＰ間認証におけるＡＰ側の認証処理のフローチャート。

【図１３】第１の実施の形態において実施するＭＴ－ＡＳ間認証におけるＭＴ側の認証処理のフローチャート。

【図１４】第１の実施の形態において実施するＭＴ－ＡＳ間認証におけるＡＳ側の認証処理のフローチャート。

【図１５】第１の実施の形態において実施するＭＴ－ＡＳ間認証におけるＡＰ側の認証結果２以外のパケット受信時の認証処理のフローチャート。

【図１６】第１の実施の形態において実施するＭＴ－ＡＳ間認証におけるＡＰ側の認証結果２のパケット受信時の認証処理のフローチャート。

【図１７】本発明の第２の実施の形態の無線アクセスネットワークにおける基地局密度が高い環境での１つの無線端末（ＭＴ）が複数の基地局（ＡＰ）と通信する状況を示す説明図。

【図１８】第２の実施の形態における無線端末の機能構成のブロック図。

【図１９】第２の実施の形態における無線端末の機能ブロック図。

【図２０】第２の実施の形態において実施するＭＴ－認証サーバ（ＡＳ）間の認証シーケンス図。

【図２１】第２の実施の形態におけるＭＴのＡＰ選択処理のフローチャート。

【図２２】本発明の第３の実施の形態の無線アクセスネットワークにおけるＭＴのＡＰ選択処理のフローチャート。

【図２３】本発明の第４の実施の形態の無線アクセスネットワークにおけるＭＴのＡＰ選択処理のフローチャート。

【図２４】本発明の第５の実施の形態の無線アクセスネットワークにおけるＭＴのＡＰ選択処理のフローチャート。

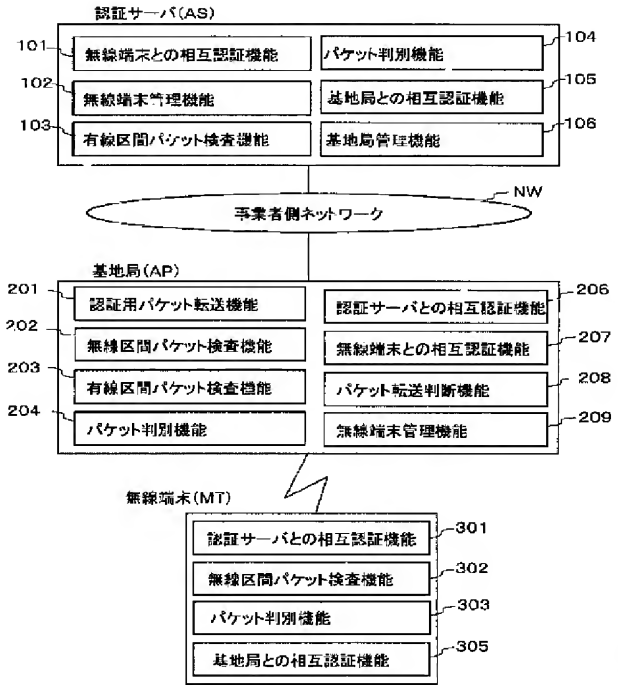
【図２５】本発明の第６の実施の形態の無線アクセスネットワークにおけるＭＴのＡＰ選択処理のフローチャート。

【図２６】本発明の第７の実施の形態の無線アクセスネットワークにおけるＭＴのＡＰ選択処理のフローチャート。

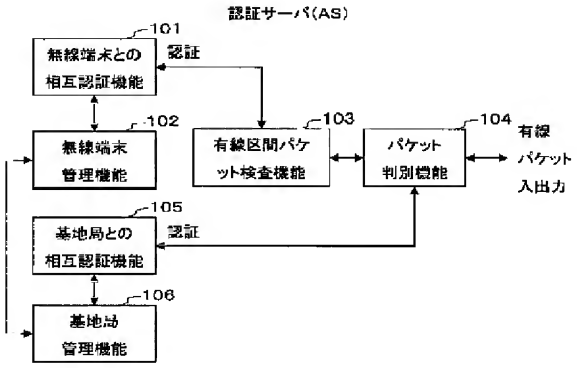
【図２７】本発明の第８の実施の形態の無線アクセスネ

ットワークにおける認証サーバ（ＡＳ）の機能構成のブロック図。
【図２８】第８の実施の形態における基地局（ＡＰ）の機能構成のブロック図。
【図２９】第８の実施の形態における認証サーバ（ＡＳ）の機能ブロック図。
【図３０】第８の実施の形態における基地局（ＡＰ）の機能ブロック図。
【図３１】第８の実施の形態によるＡＳのＡＰに対するリソース開放処理のシーケンス図。
【図３２】上記のリソース開放処理に用いるパケットフォーマットの説明図。
【図３３】第８の実施の形態におけるＡＳのＭＴ移動管理処理のフローチャート。
【図３４】本発明の第９の実施の形態の無線マルチホップネットワークの機能構成のブロック図。
【図３５】第９の実施の形態における認証サーバの機能ブロック図。
【図３６】第９の実施の形態における基地局の機能ブロック図。
【図３７】第９の実施の形態における無線端末の機能ブロック図。
【図３８】第９の実施の形態の無線アクセスネットワークの動作説明図。
【図３９】第９の実施の形態において実施する無線端末（ＭＴ）－認証サーバ（ＡＳ）間の認証シーケンス図。
【図４０】第９の実施の形態において使用するＭＴ－ＡＳ間の認証用パケットのペイロードデータの説明図。
【図４１】第９の実施の形態において実施するＭＴ－ＭＴ間認証における新規ＭＴ側の認証処理のフローチャート。
【図４２】第９の実施の形態において実施するＭＴ－ＭＴ間認証におけるＰｒｏｘｙＭＴ側の認証処理のフローチャート。
【図４３】第９の実施の形態において実施するＭＴ－ＡＳ間認証における新規ＭＴ側の認証処理のフローチャート。
【図４４】第９の実施の形態において実施するＭＴ－ＡＳ間認証におけるＡＳ側の認証処理のフローチャート。
【図４５】第９の実施の形態において実施するＭＴ－ＡＳ間認証におけるＰｒｏｘｙＭＴ側又は基地局（ＡＰ）側の認証２用パケット受信時の認証処理のフローチャート。
【図４６】第９の実施の形態において実施するＭＴ－ＡＳ間認証における中継ＭＴ側のパケット中継処理のフローチャート。
【図４７】本発明の第１０の実施の形態の無線マルチホップネットワークにおいて実施するＭＴ間認証における新規ＭＴ側の認証処理のフローチャート。
【図４８】本発明の第１１の実施の形態の無線マルチホップネットワークにおいて実施するＭＴ間認証における新規ＭＴ側の認証処理のフローチャート。
【図４９】本発明の第１２の実施の形態の無線マルチホップネットワークにおいて実施するＭＴ間認証における新規ＭＴ側の認証処理のフローチャート。
【図５０】従来から提案されている無線アクセスネットワークの機能構成のブロック図。
【図５１】従来から提案されている無線アクセスネットワークに対するＤｏＳ攻撃の説明図。
【図５２】従来から提案されている無線アクセスネットワークにおける認証処理の多重発生のメカニズムの説明図。
【図５３】従来から提案されている無線マルチホップネットワークの機能構成のブロック図。
【図５４】従来から提案されている無線マルチホップネットワークにおける認証処理の多重発生のメカニズムの説明図。
【符号の説明】
１０１　無線端末との相互認証機能
１０２　無線端末管理機能
１０３　有線区間パケット検査機能
１０４　パケット判別機能
１０５　基地局との相互認証機能
１０６　基地局管理機能
１０７　無線端末移動管理機能
２０１　認証用パケット転送機能
２０２　無線区間パケット検査機能
２０３　有線区間パケット検査機能
２０４　パケット判別機能
２０５　パケット中継機能
２０６　認証サーバとの相互認証機能
２０７　無線端末との相互認証機能
２０８　パケット転送判断機能
２０９　無線端末管理機能
２１０　リソース開放機能
３０１　認証サーバとの相互認証機能
３０２　無線区間パケット検査機能
３０３　パケット判別機能
３０４　パケット中継機能
３０５　基地局との相互認証機能
３０７　無線端末との相互認証機能
３０８　無線端末選択機能
３０９　パケット転送機能
ＡＳ　認証サーバ（Ａｕｔｈｅｎｔｉｃａｔｉｏｎ　Ｓｅｒｖｅｒ）
ＡＰ　基地局（Ａｃｃｅｓｓ　Ｐｏｉｎｔ）
ＭＴ　無線端末（Ｍｏｂｉｌｅ　Ｔｅｒｍｉｎａｌ）
ＮＷ　（有線）事業者用ネットワーク

【図1】

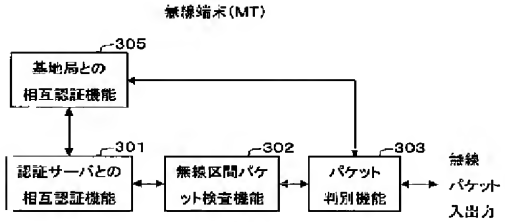


【図2】



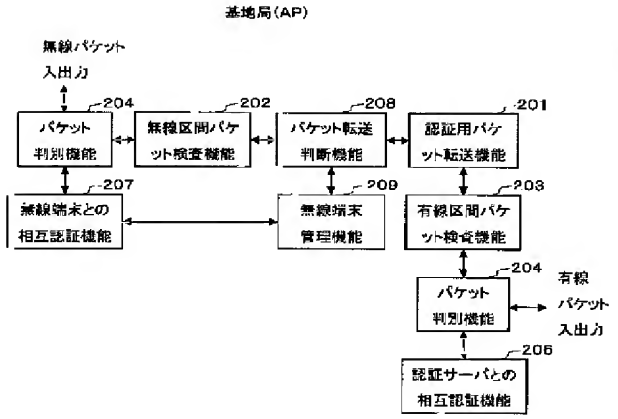
【図3】

【図4】

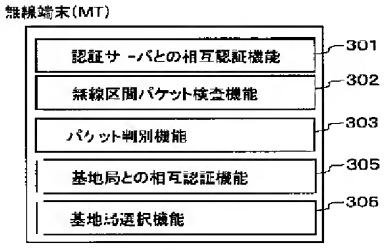


【図18】

【図32】



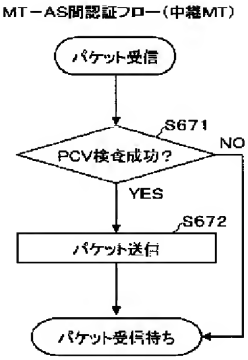
【図5】



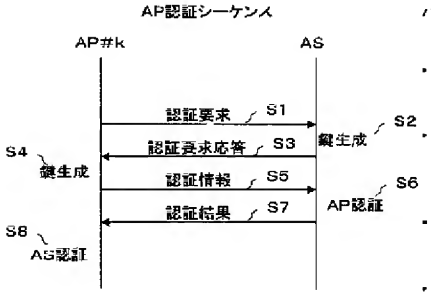
パケットフォーマット

- リソース開放通知
  AS、AP1、MT
- リソース開放完了
  AP1、AS、MT、Info

【図46】



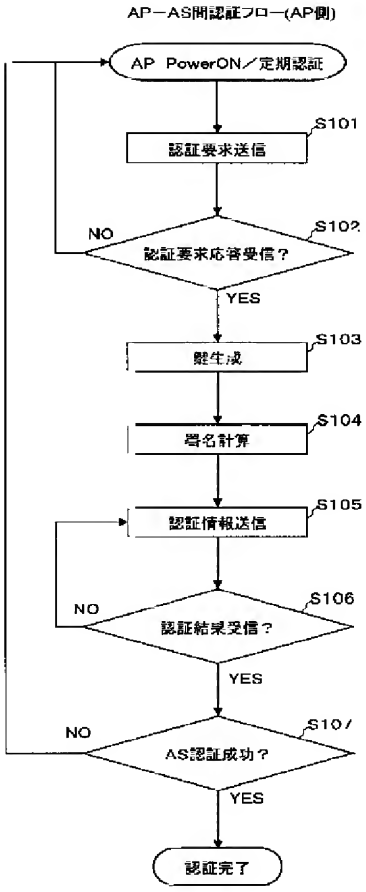
【図6】



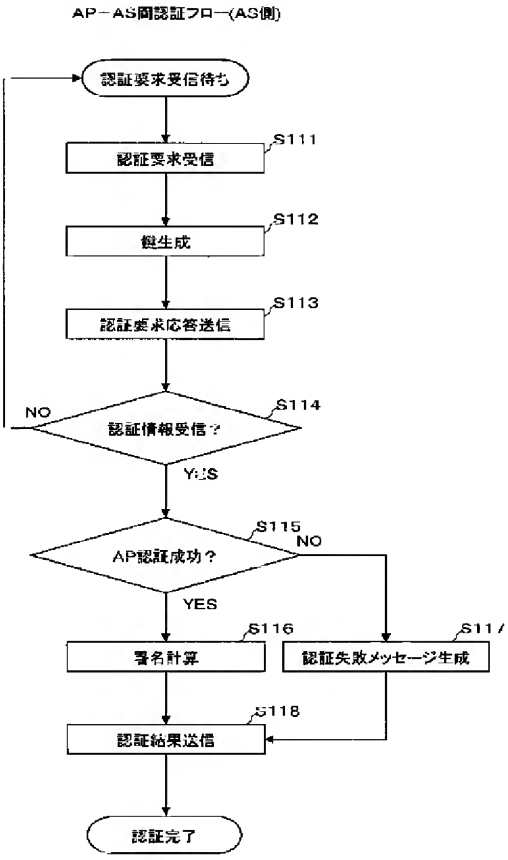
パケットペイロードデータ

- 認証要求応答
  - AS、KE as、R1
- 認証情報
  - AP#k、R2、Cert#k、Sig#k
  - Sig#k=EP(SK#k、H(AP#k、AS、R1、KE ap#k、KE as))
- 認証結果
  - AP#k、Cert ap#k、Sig ap#k
  - Sig as=EP(SK as、H(AS、AP#k、R2、KE as、KE ap#k)
- 認証要求
  - AP#k、KE ap#k

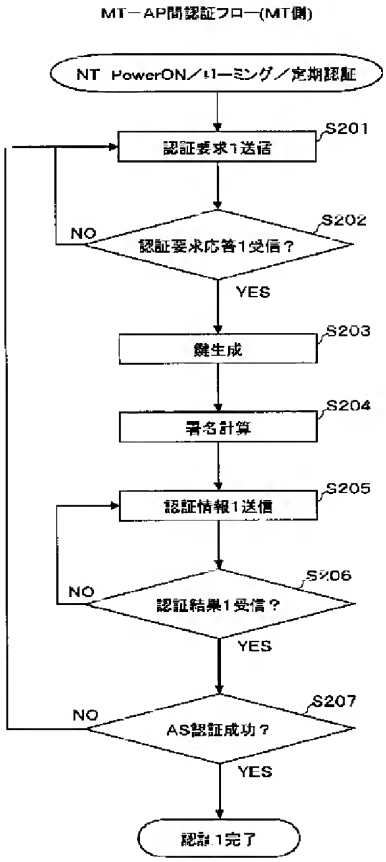
【図7】



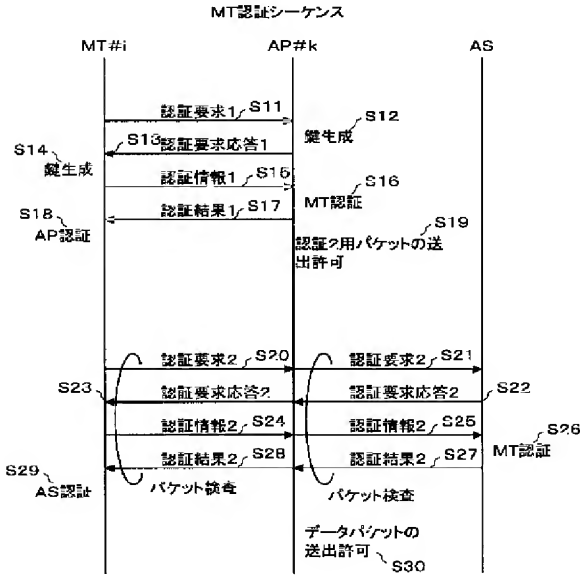
【図8】



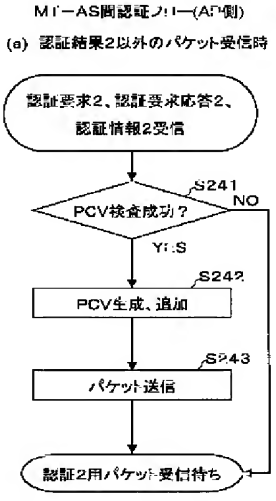
【図11】



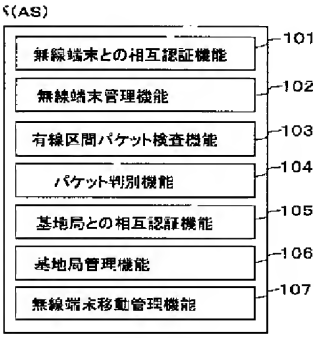
【図9】



【図15】



【図27】



【図10】

パケットペイロードデータ

認証要求1
MT#i, KE mt#i

認証要求応答1
AP#k, Ki ap#k, R1

認証情報1
MT#i, R2, Cert mt#i, Sig mt#i
Sig mt#i=EP(SK mt#i, H(MT#k, AP#k, R1, KE mt#i, KE ap#k))

認証結果1
AP#k, Cert ap#k, Sig ap#k
Sig ap#k=EP(SK ap#k, H(AP#k, MT #k, R2, Ki ap#k, KE mt#i))

認証要求2
MT#i, AP#k+PCV

認証要求応答2
AS, MT#i, AP#k, R3+PCV

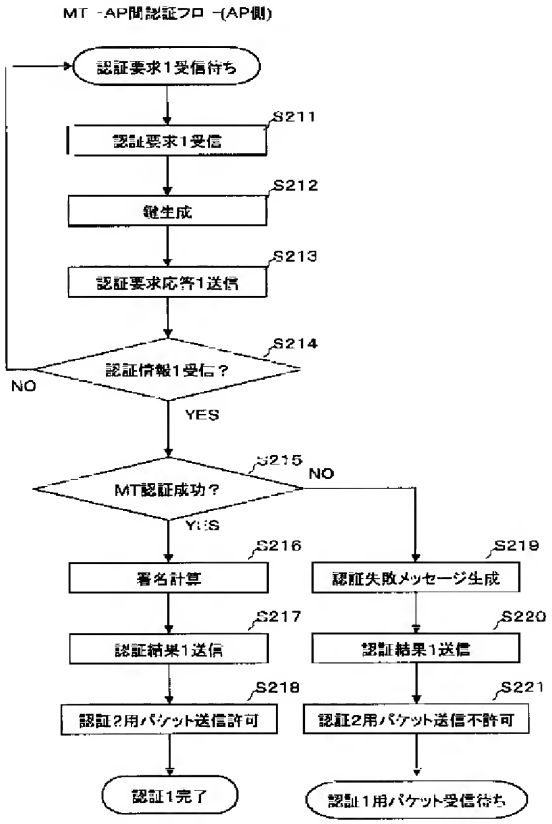
認証情報2
MT#i, AP#k, Cert mt#i, Sig mt#i+PCV
Sig mt#i=EP(SK mt#i, H(MT#i, AP#k, AS, R3))

認証結果2
AS, MT#i, AP#k, Cert as, Sig as+PCV
Sig as=EP(SK as, H(AS, MT#i, AP#k, R4))

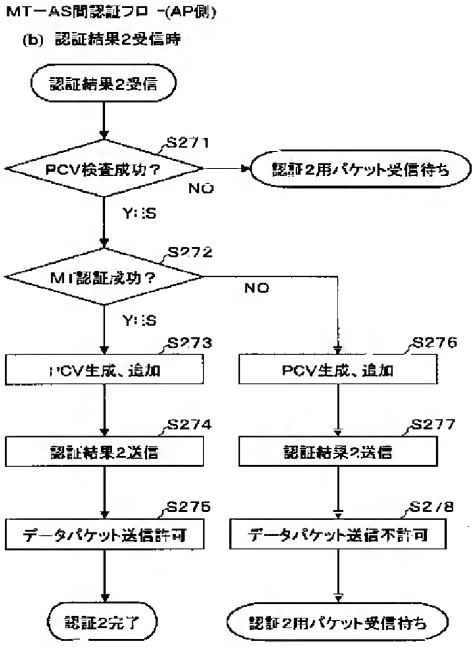
認証2用パケット検査データ(PCV)
MT−AP間:
MT用: PCV=SQN+EP(SK mt#i, H(data, SQN))
AP用: PCV=SQN+EP(SK ap#k, H(data, SQN))
AP−AS間:
PCV=SQN+ES(K ap#k−as, H(data, SQN))

EP:公開鍵暗号
ES:共有鍵暗号
PK, SK:公開鍵、秘密鍵
KE:鍵生成情報
H:ハッシュ関数
SQN:シーケンス番号
R:乱数
K:個別鍵(共有鍵)
Cert:証明書
Sig:ディジタル署名
PCV:パケット検査データ

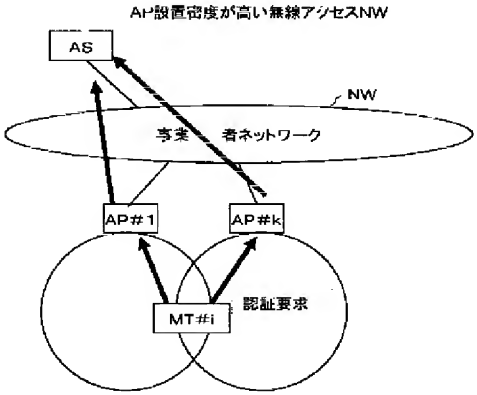
【図12】



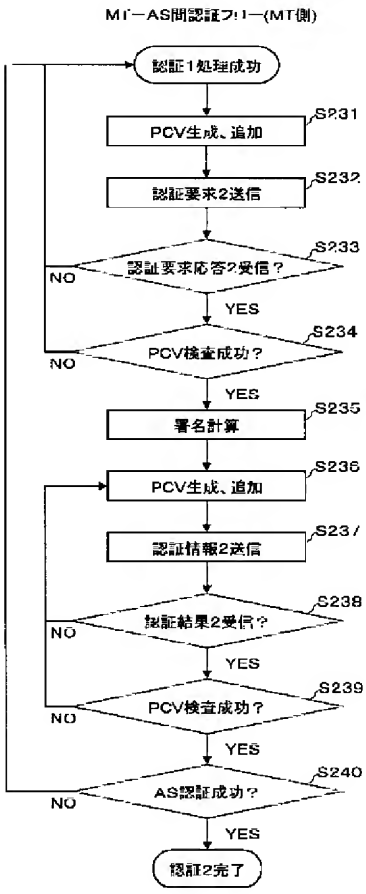
【図16】



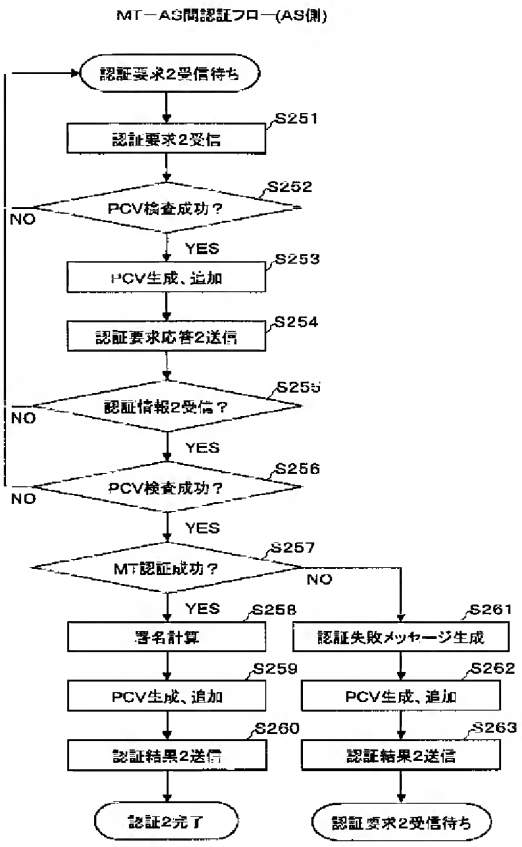
【図17】



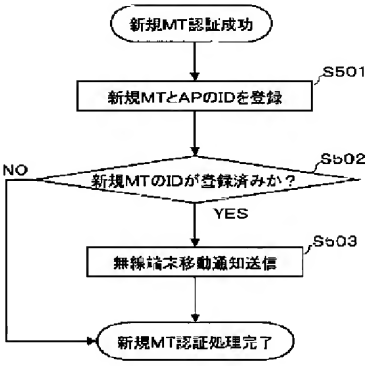
【図13】



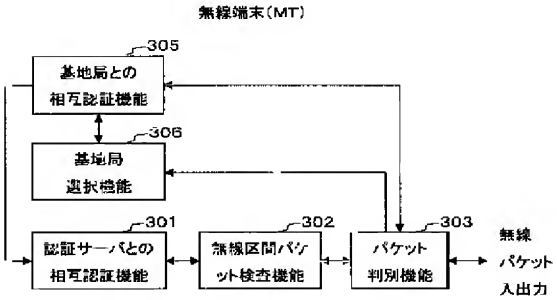
【図14】



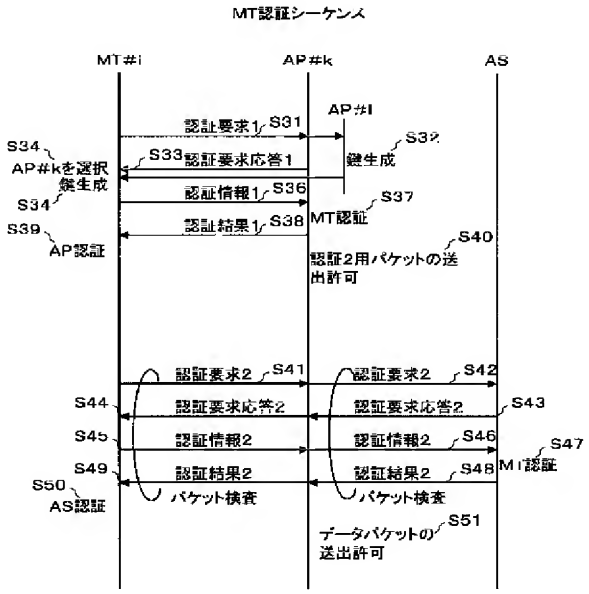
【図33】



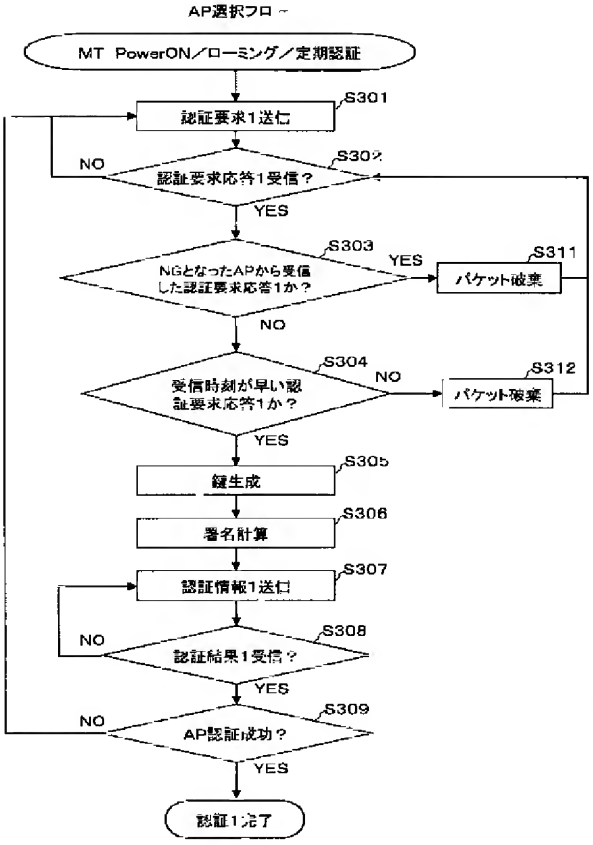
【図19】



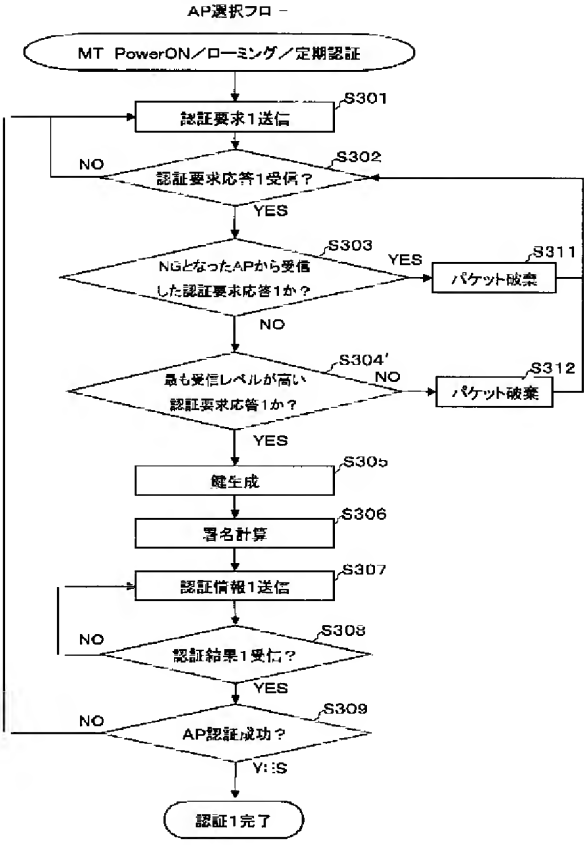
【図20】



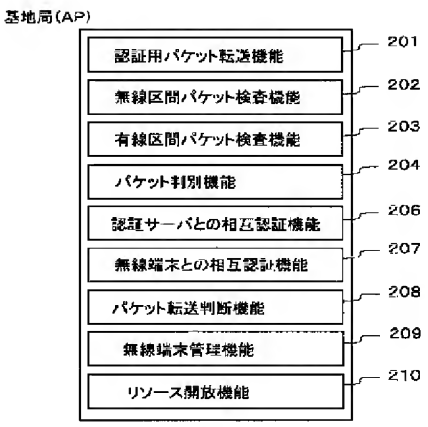
【図21】



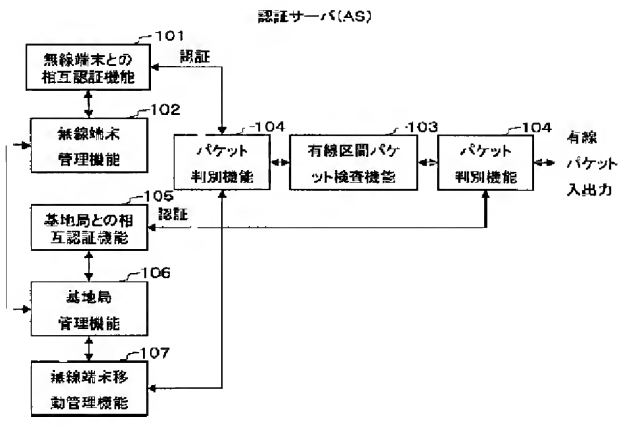
【図22】



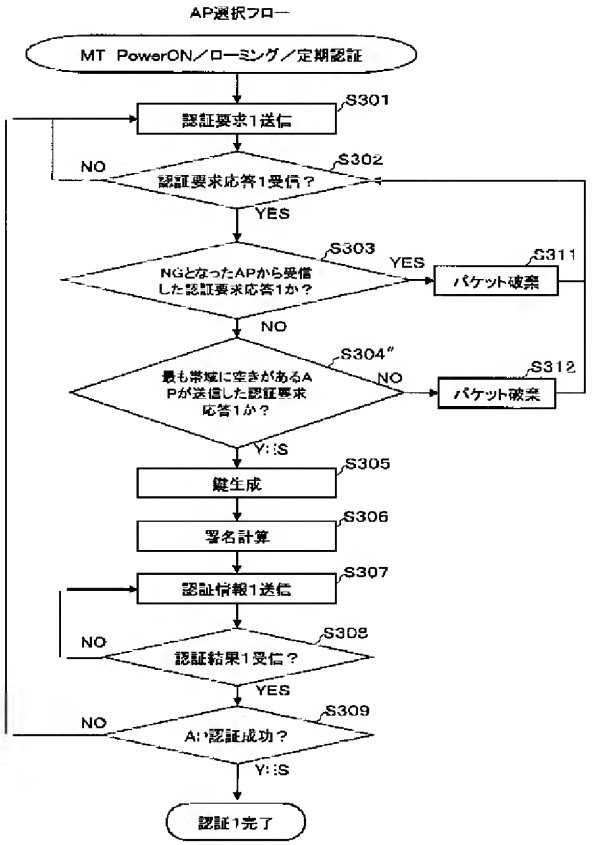
【図28】



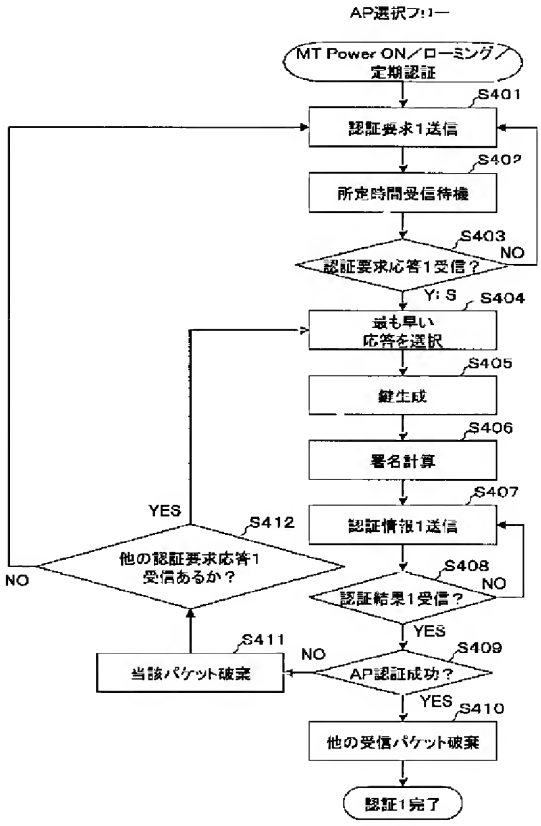
【図29】



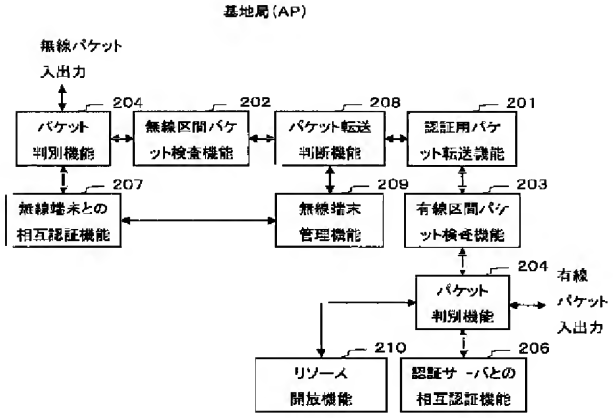
【図23】



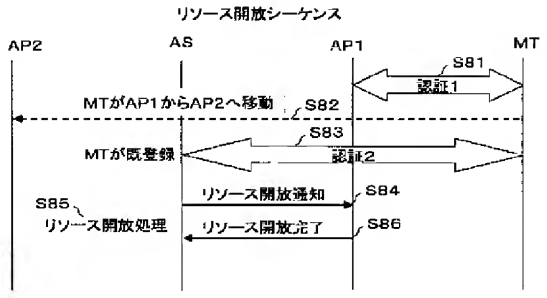
【図24】



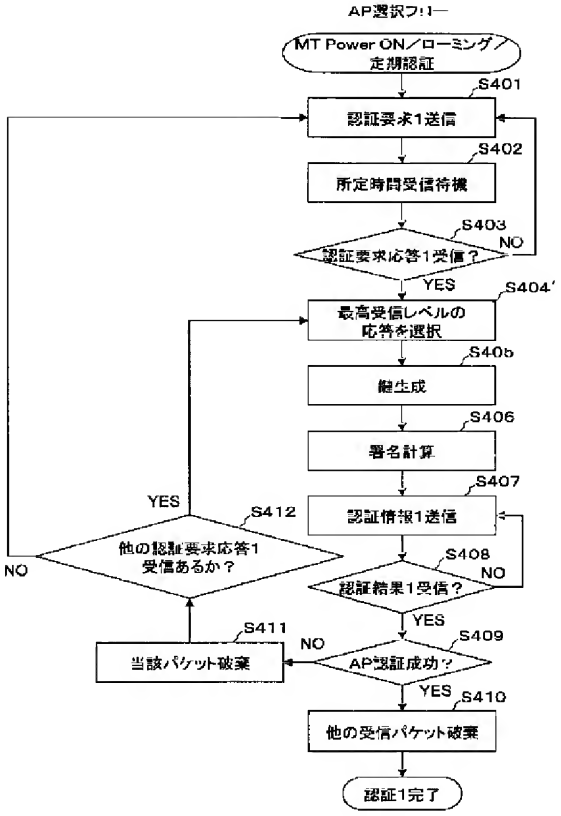
【図30】



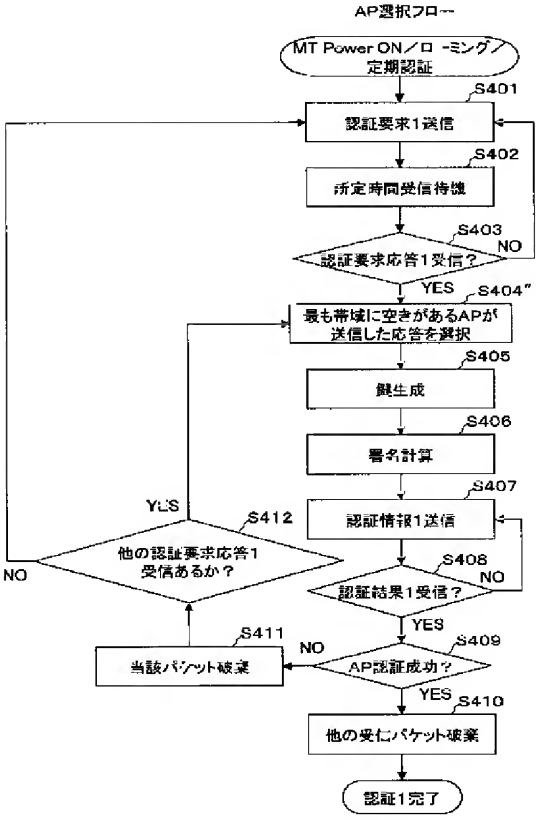
【図31】



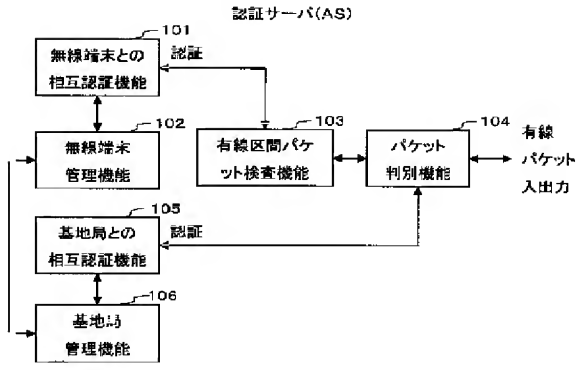
【図25】



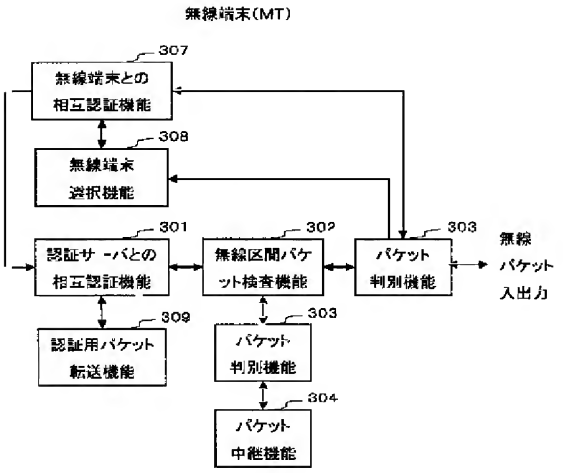
【図26】



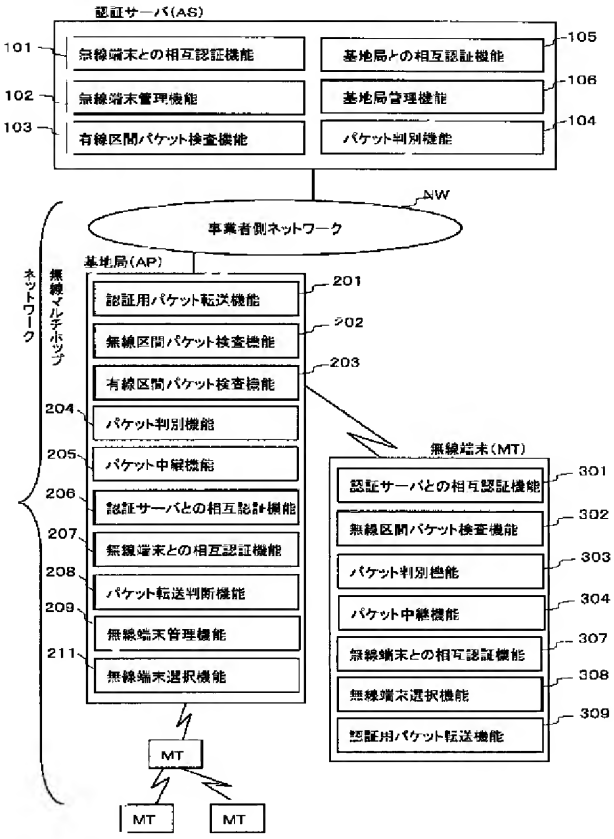
【図35】



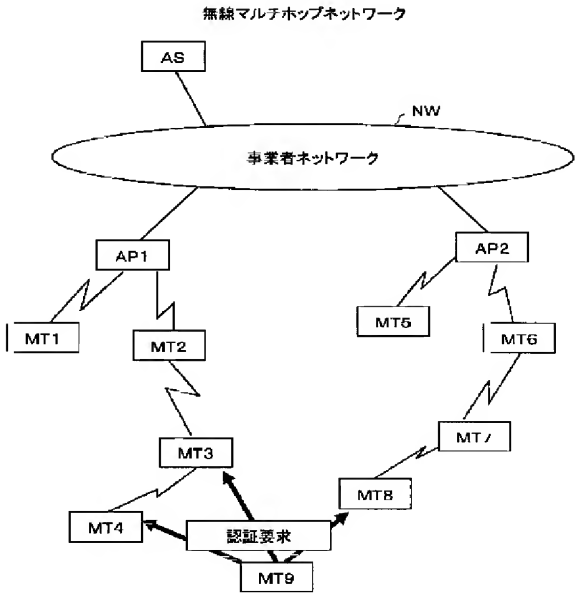
【図37】



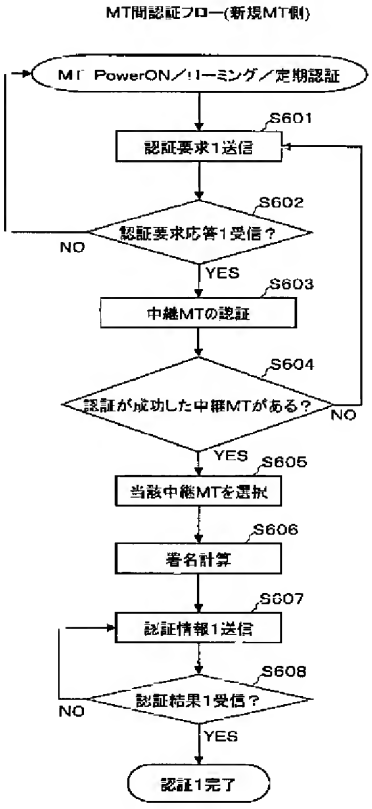
【図34】



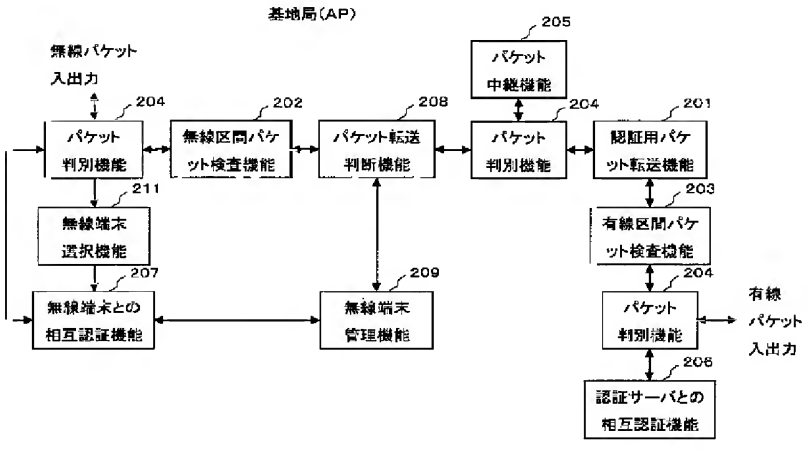
【図38】



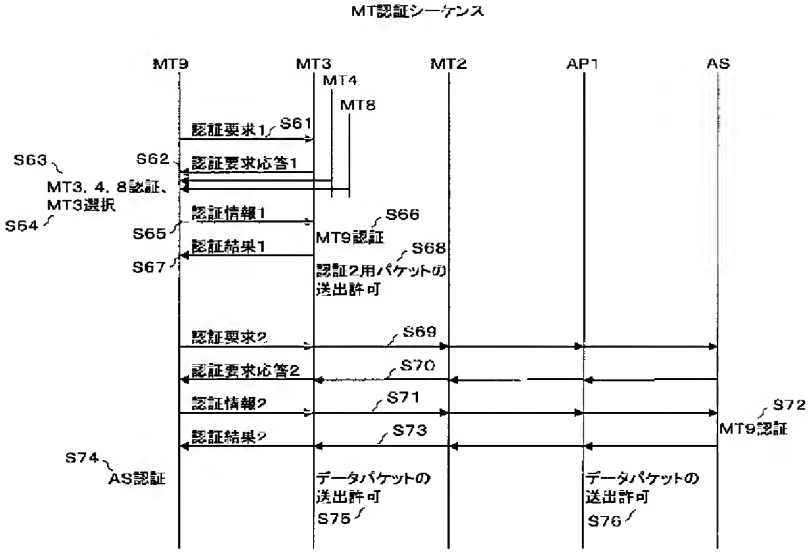
【図41】



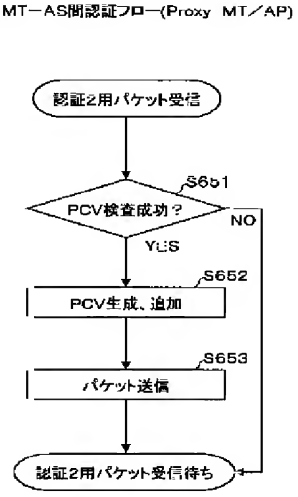
【図36】



【図39】



【図45】



【図40】

パケットペイロードデータ

認証要求1
MT9, R1

認証要求応答1
MT3, R2, Cert mt3, Sig mt3, RInfo
Sig mt3=EP(SK mt3, H(MT3, MT9, R1, RInfo))

認証情報1
MT9, Cert mt9, Sig mt9
Sig mt9=EP(SK mt9, H(MT9, MT3, R2))

認証結果1
MT3, MT9

認証要求2
MT3, AP1+PCV

認証要求応答2
AS, MT9, AP1, R3+PCV

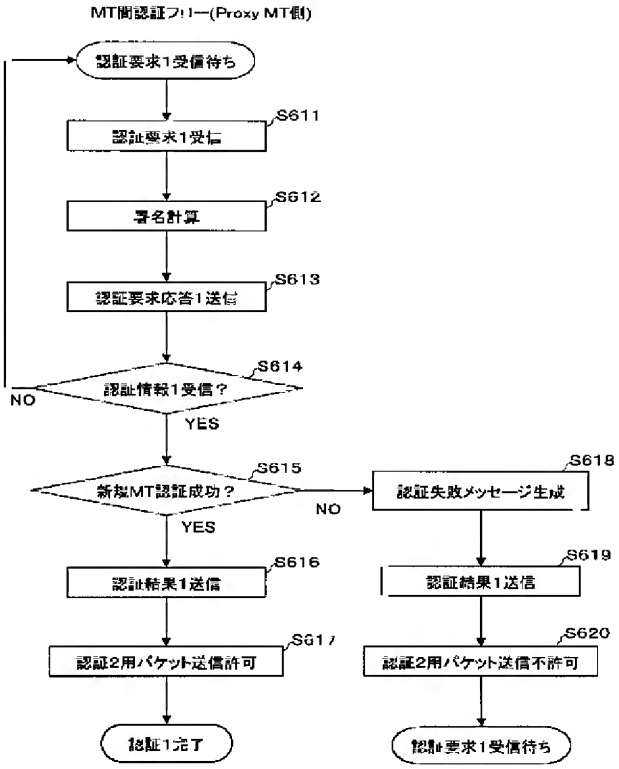
認証情報2
MT9, AP1, R4, Cert mt9, Sig mt9+PCV
Sig mt9=EP(SK mt9, H(MT9, AP1, AS, R3))

認証結果2
AS, MT9, AP1, Cert as, Sig as, [NK]+PCV
Sig as :EP(SK as, H(AS, MT9, AP1, R4))
{NK}=EP(PK mt9, NK)

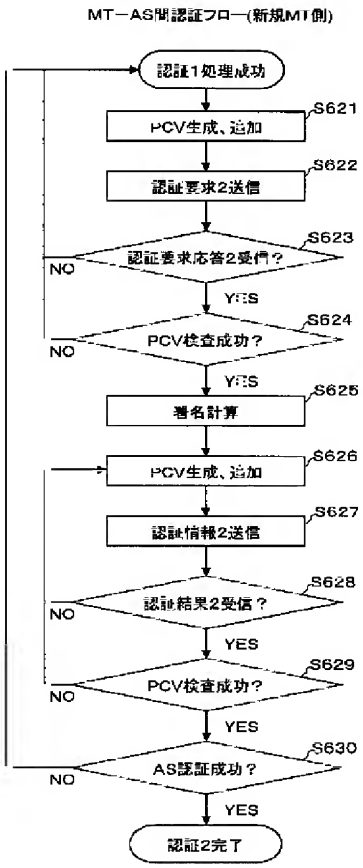
認証2用パケット検査データ(PCV)
MT9−MT3間:
MT用: PCV=SQN+EP(SK mt9, H(data, SQN))
AP用: PCV=SQN+EP(SK mt3, H(data, SQN))
MT3−AP1間:
PCV=SQN+ES(NK, H(data, SQN))
AP1−AS間:
PCV=SQN+ES(K as1−as, H(data, SQN))

EP:公開鍵暗号
ES:共有鍵暗号
PK, SK:公開鍵、秘密鍵
H:ハッシュ関数
SQN:シーケンス番号
R:乱数
K:個別鍵(共有鍵)
NK:ネットワーク鍵(共有鍵)
Cert:証明書
Sig:ディジタル署名
PCV:パケット検査データ

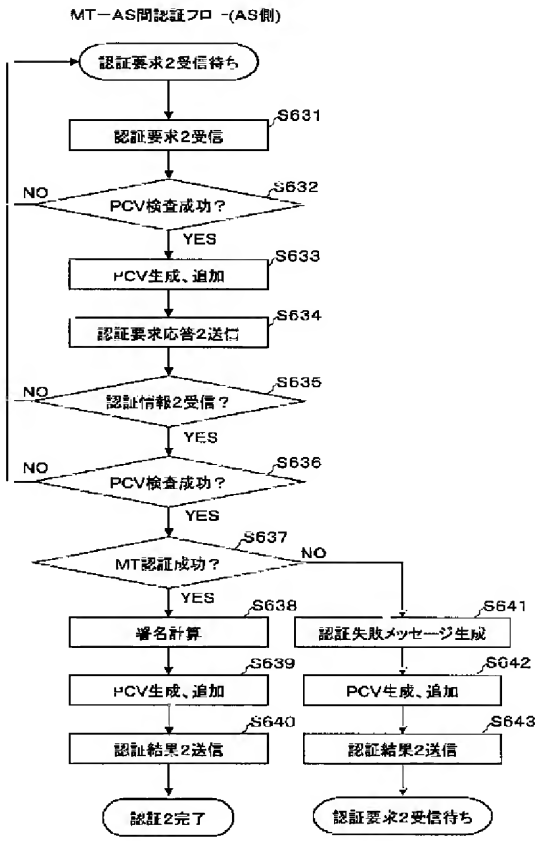
【図42】



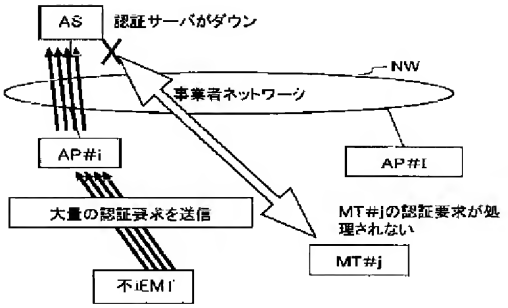
【図43】



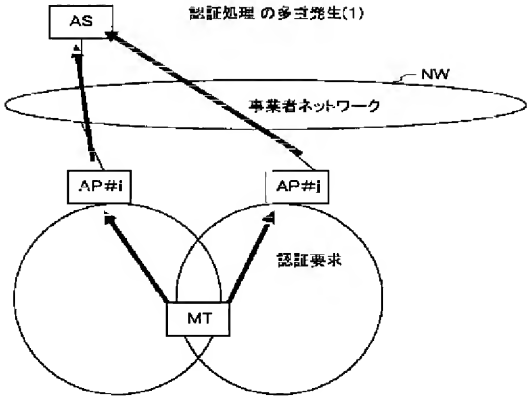
【図44】



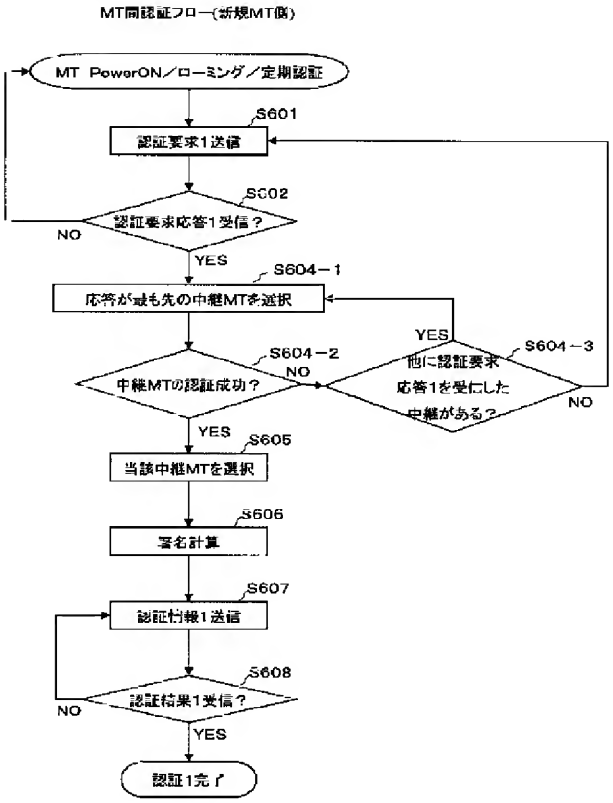
【図51】



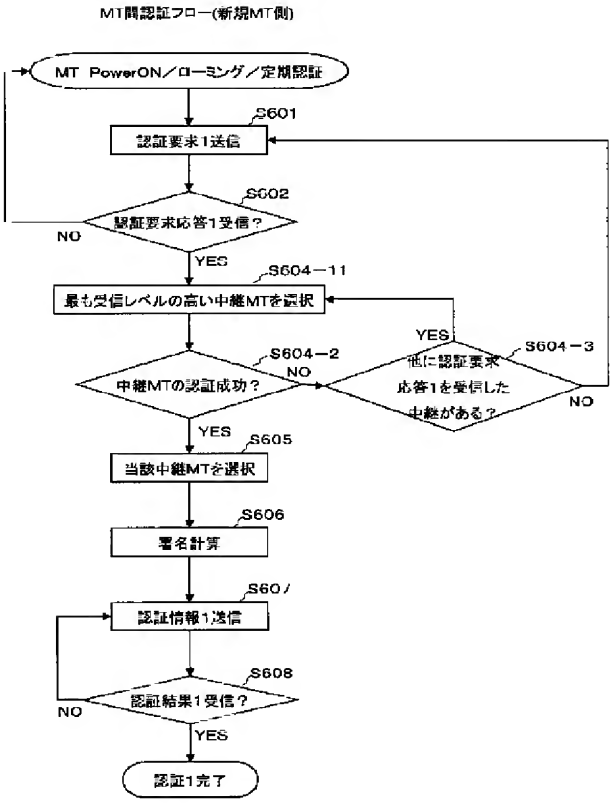
【図52】



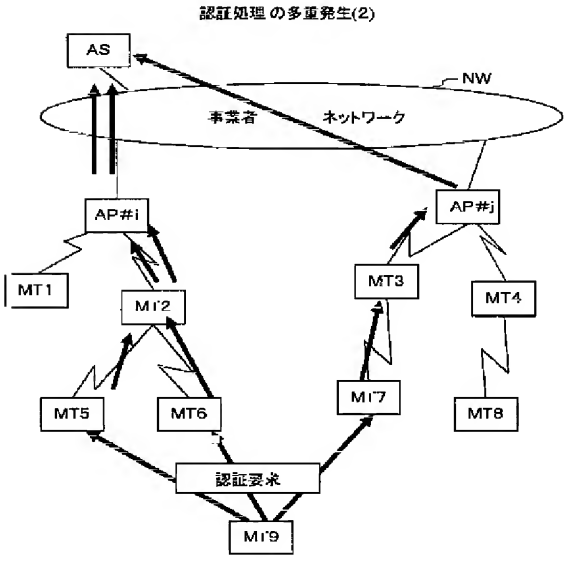
【図47】


MT間認証フロー(新規MT側)
MT PowerON/ローミング/定期認証
S601
認証要求1送信
S602
認証要求応答1受信?
NO
YES
S604-1
応答が最も先の中継MTを選択
S604-2
中継MTの認証成功?
NO
YES
S604-3
他に認証要求
応答1を受信した
中継がある?
YES
NO
S605
当該中継MTを選択
S606
署名計算
S607
認証情報1送信
S608
認証結果1受信?
NO
YES
認証1完了

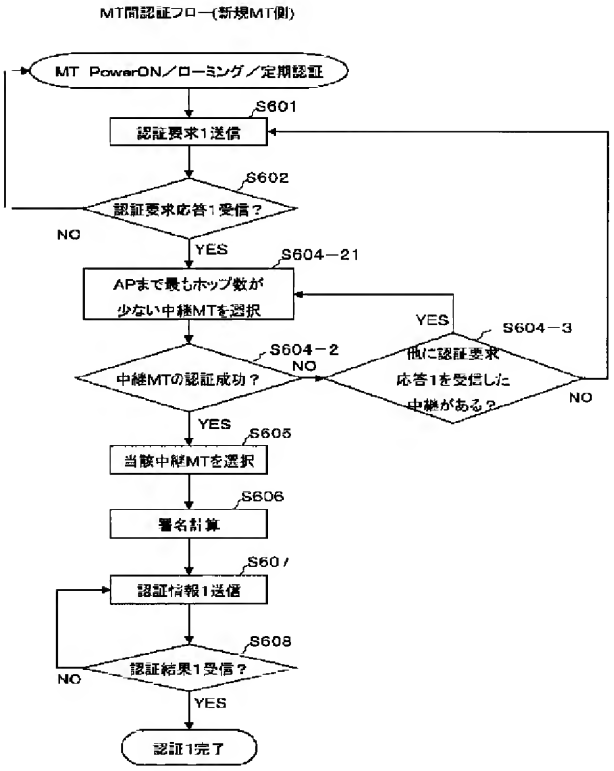
【図48】


MT間認証フロー(新規MT側)
MT PowerON/ローミング/定期認証
S601
認証要求1送信
S602
認証要求応答1受信?
NO
YES
S604-11
最も受信レベルの高い中継MTを選択
S604-2
中継MTの認証成功?
NO
YES
S604-3
他に認証要求
応答1を受信した
中継がある?
YES
NO
S605
当該中継MTを選択
S606
署名計算
S607
認証情報1送信
S608
認証結果1受信?
NO
YES
認証1完了

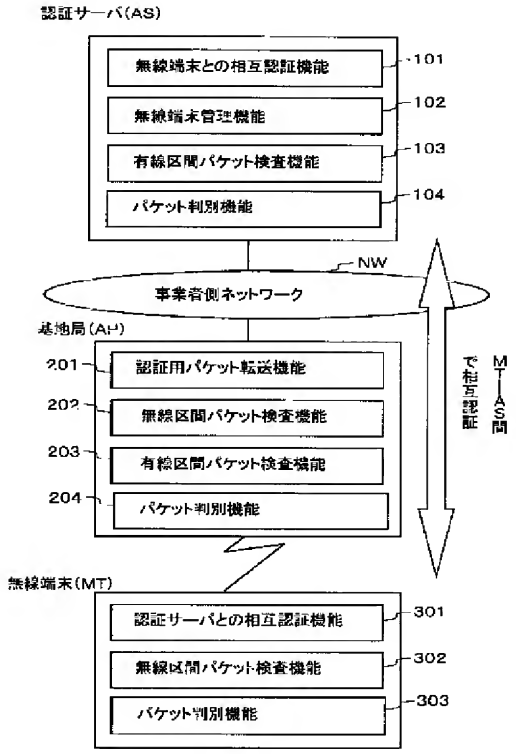
【図54】


認証処理の多重発生(2)
AS
NW
事業者
ネットワーク
AP#i
AP#j
MT1
MT2
MT3
MT4
MT5
MT6
MT7
MT8
認証要求
MT9

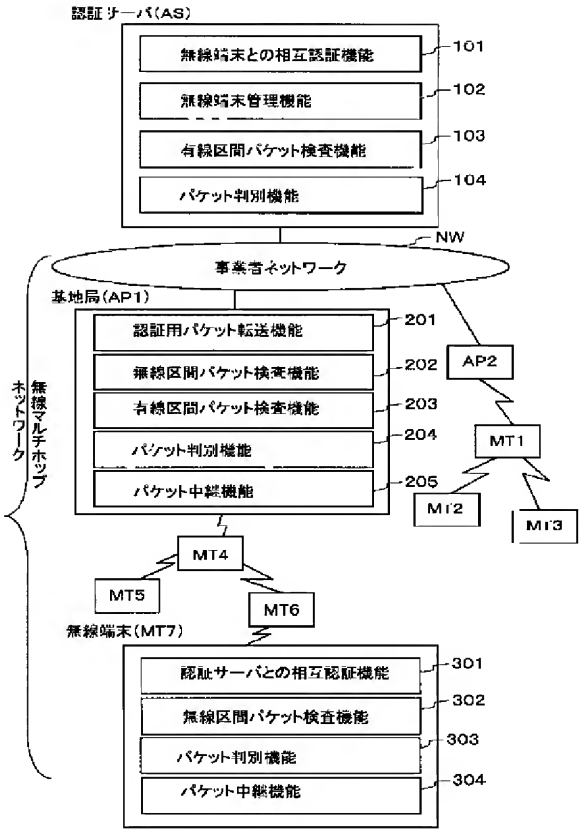
【図49】


MT間認証フロー(新規MT側)
MT PowerON/ローミング/定期認証
S601
認証要求1送信
S602
認証要求応答1受信?
NO
YES
S604-21
APまで最もホップ数が少ない中継MTを選択
S604-2
中継MTの認証成功?
NO
YES
S604-3
他に認証要求応答1を受信した中継がある?
YES
NO
S605
当該中継MTを選択
S606
署名計算
S607
認証情報1送信
S608
認証結果1受信?
NO
YES
認証1完了

【図50】


認証サーバ(AS)
無線端末との相互認証機能
101
無線端末管理機能
102
有線区間パケット検査機能
103
パケット判別機能
104
NW
事業者側ネットワーク
基地局(AP)
201
認証用パケット転送機能
202
無線区間パケット検査機能
203
有線区間パケット検査機能
204
パケット判別機能
MT-AS間で相互認証
無線端末(MT)
認証サーバとの相互認証機能
301
無線区間パケット検査機能
302
パケット判別機能
303

【図５３】



フロントページの続き

(72)発明者　中山　正芳
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

(72)発明者　須田　博人
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

Ｆターム(参考)　5J104 AA07 KA02 MA01 PA07
5K030 GA15 HA08 JL01 JT09 LB05
5K067 AA32 BB02 BB21 CC08 DD17
EE02 EE10 HH22 HH24 HH36